COMPUTER INSECURITIES AT DOE HEADQUARTERS: DOE's FAILURE TO GET ITS OWN CYBER HOUSE IN ORDER

HEARING

BEFORE THE

SUBCOMMITTEE ON
OVERSIGHT AND INVESTIGATIONS

OF THE

COMMITTEE ON COMMERCE
HOUSE OF REPRESENTATIVES

ONE HUNDRED SIXTH CONGRESS

SECOND SESSION

JUNE 13, 2000

Serial No. 106–157

Printed for the use of the Committee on Commerce

U.S. GOVERNMENT PRINTING OFFICE
65–910CC WASHINGTON : 2000

COMMITTEE ON COMMERCE

TOM BLILEY, Virginia, *Chairman*

W.J. "BILLY" TAUZIN, Louisiana
MICHAEL G. OXLEY, Ohio
MICHAEL BILIRAKIS, Florida
JOE BARTON, Texas
FRED UPTON, Michigan
CLIFF STEARNS, Florida
PAUL E. GILLMOR, Ohio
Vice Chairman
JAMES C. GREENWOOD, Pennsylvania
CHRISTOPHER COX, California
NATHAN DEAL, Georgia
STEVE LARGENT, Oklahoma
RICHARD BURR, North Carolina
BRIAN P. BILBRAY, California
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
CHARLIE NORWOOD, Georgia
TOM A. COBURN, Oklahoma
RICK LAZIO, New York
BARBARA CUBIN, Wyoming
JAMES E. ROGAN, California
JOHN SHIMKUS, Illinois
HEATHER WILSON, New Mexico
JOHN B. SHADEGG, Arizona
CHARLES W. "CHIP" PICKERING, Mississippi
VITO FOSSELLA, New York
ROY BLUNT, Missouri
ED BRYANT, Tennessee
ROBERT L. EHRLICH, Jr., Maryland

JOHN D. DINGELL, Michigan
HENRY A. WAXMAN, California
EDWARD J. MARKEY, Massachusetts
RALPH M. HALL, Texas
RICK BOUCHER, Virginia
EDOLPHUS TOWNS, New York
FRANK PALLONE, Jr., New Jersey
SHERROD BROWN, Ohio
BART GORDON, Tennessee
PETER DEUTSCH, Florida
BOBBY L. RUSH, Illinois
ANNA G. ESHOO, California
RON KLINK, Pennsylvania
BART STUPAK, Michigan
ELIOT L. ENGEL, New York
TOM SAWYER, Ohio
ALBERT R. WYNN, Maryland
GENE GREEN, Texas
KAREN McCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DeGETTE, Colorado
THOMAS M. BARRETT, Wisconsin
BILL LUTHER, Minnesota
LOIS CAPPS, California

JAMES E. DERDERIAN, *Chief of Staff*
JAMES D. BARNETTE, *General Counsel*
REID P.F. STUNTZ, *Minority Staff Director and Chief Counsel*

SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS

FRED UPTON, Michigan, *Chairman*

JOE BARTON, Texas
CHRISTOPHER COX, California
RICHARD BURR, North Carolina
Vice Chairman
BRIAN P. BILBRAY, California
ED WHITFIELD, Kentucky
GREG GANSKE, Iowa
ROY BLUNT, Missouri
ED BRYANT, Tennessee
TOM BLILEY, Virginia,
(Ex Officio)

RON KLINK, Pennsylvania
HENRY A. WAXMAN, California
BART STUPAK, Michigan
GENE GREEN, Texas
KAREN McCARTHY, Missouri
TED STRICKLAND, Ohio
DIANA DeGETTE, Colorado
JOHN D. DINGELL, Michigan,
(Ex Officio)

CONTENTS

(III)

COMPUTER INSECURITIES AT DOE HEADQUARTERS: DOE's FAILURE TO GET ITS OWN CYBER HOUSE IN ORDER

TUESDAY, JUNE 13, 2000

HOUSE OF REPRESENTATIVES,
COMMITTEE ON COMMERCE,
SUBCOMMITTEE ON OVERSIGHT AND INVESTIGATIONS,
Washington, DC.

The subcommittee met, pursuant to notice, at 9:10 a.m., in room 2123, Rayburn House Office Building, Hon. Fred Upton (chairman) presiding.

Members present: Representatives Upton, Burr, Bilbray, Bryant, Bliley, (ex officio), Stupak, Green, and DeGette.

Also present: Representative Wilson.

Staff present: Tom Dilenge, majority counsel; Anthony Habib, legislative clerk; Clay Alspach, legislative clerk; Edith Holleman, minority counsel; and Brendan Kelsay, minority research analyst.

Mr. UPTON. Good morning, everyone and welcome.

Today's alarming news story may change the focus of this morning's hearing a little bit. Americans everywhere want absolute assurances that our nuclear secrets remain just that, secret.

Sadly, today's headlines are indeed startling regarding the missing disks and the unsuccessful attempts of answering the many questions that are now out there. How can these disks be missing after more than a month with only as many as 86 individuals, 26 being unescorted, having access to these highly classified disks?

Real security is going to require additional changes in how DOE and its labs control their classified data, whether in hard copy or on computer disk. Our hearing today, coupled with this news from Los Alamos, shows how far the Department, in its lapse, still must go to make security the priority that everyone wants it to be.

This subcommittee will hold a hearing to continue its year-long review of cyber security practices at the Department of Energy. This time, our focus is not on the Department's nuclear weapons labs—which have received the lion's share of attention and have made real improvements in computer security since last year—but on DOE headquarters itself. Unfortunately, the current situation at DOE headquarters is little better than where the labs were a year ago, a startling and troubling revelation given the Secretary's professed commitment over 1 year ago to make security, and cyber security in particular, a top priority throughout the Department.

We'll hear today once again from Mr. Glenn Podonsky, whose office conducts independent reviews of DOE security practices, including the latest audit of headquarters cyber security completed last month. At our last hearing on DOE's security issues, Mr. Podonsky's office promised in response to Congresswoman Wilson's questioning to initiate an expedited review of headquarters cyber security, and I am pleased that he's with us to report to the subcommittee on the findings of this audit. In particular, we will hear that the headquarters computer network has many significant and easily exploitable vulnerabilities that render it both susceptible to internal and external threats.

As with the labs, we will hear once again about the lack of internal security controls to limit the ability of authorized and unauthorized users, including some foreign nationals, to move freely among the various program office systems to compromise sensitive information. On this unified network is not only the Secretary's office but also key program functions, such as defense programs, nonproliferation and national security, security operations, counterintelligence, the general counsel and inspector general, and even Mr. Podonsky's office. While these offices' classified data is physically separate from the unclassified network, the audit does raise concerns about whether the tighter controls that were ordered more than a year ago by the Secretary to limit the transfer of classified data to the unclassified systems have in fact been implemented at DOE's own headquarters.

As with the labs, we'll also hear about deficiencies in certain fire walls and intrusion detection systems. While no Internet fire wall is ever 100 percent foolproof, it is important that a sytem be able to quickly detect and block this spread of unauthorized entries into the network. By this important measure, DOE falls significantly short of the mark.

From a management perspective, the audit essentially finds that no single person or entity is in charge of this network, an amazing finding in and of itself, and most likely the root cause of the technical problems uncovered by this audit. It appears that much like other Federal agencies the committee has looked at, the chief information officer at DOE is the chief in name only.

Given Secretary Richardson's reorganization last summer, which elevated the CIO and gave him responsibility for all cyber security efforts throughout the Department, I would have thought that the CIO would have also received the authority to mandate certain minimum requirements and corrective actions to vulnerable systems. Instead, we now find out that the CIO lacks, according to the audit, "real and perceived authority to order changes," a view apparently shared by the CIO himself.

I know I must speak for many members of this committee when I say that I find the whole situation bewildering. How could DOE headquarters, which was the catalyst for the security changes at the nuclear weapons labs last year, leave its own systems so vulnerable to misuse; and why is the Department's CIO so powerless to change the situation?

These and many other questions will be explored at today's hearing, and I welcome our panel of witnesses. In particular, I look forward to the testimony of General Habiger, DOE's security czar, and Mr. Gilligan, DOE's CIO, on what technical and management changes DOE intends to make to fix these serious problems and on what timetable. I am glad to see that after we'd noticed this hearing last week, the Department immediately moved to give this CIO new powers over the headquarters network; and I hope he uses that power to quickly and effectively gain control over this important cyber system.

At this point, I yield to my friend from Michigan, Mr. Stupak, the acting ranking member for this morning's hearing.

Mr. STUPAK. Thanks, Mr. Chairman, and thanks for holding this important hearing.

Yesterday, I was prepared to give an opening statement regarding cyber security at the Department of Energy, but after reading the New York Times yesterday, I was forced to substantially change my statement.

I'm very concerned that the Department of Energy has no idea what happened to two hard drives containing classified information about our nuclear weapons program. According to the New York Times, the hard drives contained detailed specifications about U.S. and Russian nuclear weapons. However, what is more concerning is the laissez-faire attitude Los Alamos National Laboratory and the Department of Energy have displayed in trying to ascertain what happened to highly classified information.

In the article, a senior Energy official is quoted as saying, "In my opinion, it's premature to call this a security breach." Well, I, for one, think it is a security breach and has definitely been breached and no one can say what has happened to the hard drives, who had control of the hard drives or who last had access to them.

I have to tell you, in my hometown of Menominee, Michigan, if I want to check out a library book at the Menominee Public Library, you have to have a library card and they make a record if you remove the book; and if you keep the book too long, they send you a notice asking you to return it. Eventually, they charge you late fine. Most Americans would find it hard to believe that Menominee Public Library has a more sophisticated tracking system for "Winnie the Pooh" than Los Alamos has for highly classified nuclear weapons data. That is exactly the situation we're faced with.

Mr. Curran, the Director of the Department's Counterintelligence Office, is quoted as saying, "At this point, there is no evidence that suggests espionage is involved in this incident."

How are we going to find out? Does Mr. Curran expect someone from Baghdad or Beijing to call them next year and ask for a software update?

We need to get the answers from the witnesses on a number of issues. Why did it take Los Alamos National Laboratory 3 weeks to alert the Department of Energy that the hard drives were missing? How were these hard drives and computers stored? A couple of months ago the State Department lost highly classified information on nuclear weapons. Now Los Alamos has misplaced highly classified information. This is not a joke. We're talking about highly classified nuclear weapons data.

I have been a critic of the lack of security at our nuclear weapons laboratory at Lawrence Livermore, Los Alamos and other facilities. Other members have come to me and asked me to tone it down; I will once the national labs take the security breaches seriously.

I believe it's time to take—make security at our national labs a military priority and not a civilian afterthought.

Mr. Chairman, we need answers and we need results. While I understand the witnesses are prepared to discuss cyber security at the Department of Energy, I intend to ask questions about the latest loss of our Nation's nuclear secrets, and I hope I will get some answers to my questions today.

Thank you, Mr. Chairman.

Mr. UPTON. I recognize Mr. Bliley for an opening statement.

Chairman BLILEY. Thank you, Mr. Chairman.

Since allegations of spying at Los Alamos first surfaced early last year, this committee and the American public have been subject to a steady stream of press releases, action plans, tough talk and photo ops from Secretary Richardson and senior DOE officials, designed to show a commitment to security at the Department of Energy. They have crisscrossed the country, making lots of visits to the nuclear weapons labs, demanding reforms and upgrades to security systems, particularly computer systems; and we've been told that the Department's contractors have, "gotten the message," "zero tolerance," for poor security.

I certainly don't mean to belittle these efforts because they have had some positive effect, particularly when combined with this committee's aggressive oversight and the bright media spotlight. But despite the travels and television appearances, the Secretary apparently hasn't checked his own headquarters office. Effective leadership requires making sure your own house is in order when demanding others clean up theirs. Today, we are witnessing nothing less than a failure of leadership.

A recent internal inspection by the Department's independent cyber security team, prompted by Congresswoman Wilson's request during our last oversight hearing on this matter, has revealed real flaws in the cyber security program at the Department's own headquarters that should have been corrected a long time ago. Indeed, the Department knew about many of these flaws for some time before this latest inspection occurred yet failed to fix them. That doesn't seem like zero tolerance to me, and it highlights serious management failures.

Indeed, one of the key findings in this report is that the Department, in executing its cyber security program at headquarters, has ignored the most basic principle of computer security, that a network is only as strong as its weakest link. Individual DOE program offices essentially set their own rules on security, which results in real differences in levels of security. This situation puts the entire DOE network, which contains a large amount of sensitive information, at serious risk of compromise or misuse.

Whatever the DOE spin on this is, there can be little doubt that the latest audit of cyber security is a terrible embarrassment to the Department and to the administration. How could such a situation exist at DOE if security is really a top priority?

The audit report concludes by stating that senior management attention is needed to fix the problems plaguing the Department's cyber security system. I am not sure how much more senior we can get than the Secretary, who supposedly has been focused on security at least since the spy scandal erupted over a year ago. I think it is time he and the rest of the Department focused equal attention on eliminating risks closer to home.

Finally, I just want to say a word about the recent revelations of missing classified data from Los Alamos. It is alarming that, despite the alleged focus on security over the last year, it appears the Department of Energy and its labs still have a long way to go before the American public can or should feel confident that our nuclear secrets are safe in their hands. Several months ago, I requested the General Accounting Office conduct an investigation into whether DOE and its labs have proper procedures in place to control and account for their classified documents and electronic media. The latest news from Los Alamos suggests that, whether or not this missing data is eventually recovered, the answer is no.

Thank you, Mr. Chairman.

Mr. UPTON. Thank you, Mr. Chairman.

Mrs. Wilson.

Mrs. WILSON. I ask unanimous consent to be allowed to sit in on this hearing of the Oversight and Investigations Subcommittee.

Mr. UPTON. Without objection, so ruled.

Would the gentlelady like to make an opening statement?

Mrs. WILSON. Yes, Mr. Chairman, I would.

Thank you, Mr. Chairman, for letting me sit in on this subcommittee hearing. I am not normally on the Subcommittee on Oversight and Investigations. I have a particular interest and concern on the issue of cyber security at our national laboratories.

In fact, this hearing and the testimony that we're going to hear today is the result of an inquiry that I made at a previous hearing about security at DOE headquarters. Because as all of us know, a system is only as strong as its weakest wall. And if we focus only on cyber security of systems out on the periphery of the Department of Energy and not those at DOE headquarters, we haven't strengthened the security system in the Department of Energy.

I understand that we will hear testimony today about cyber security at the headquarters of the Department of Energy on its unclassified systems. That inquiry parallels those that have previously been made at the outer rings of the Department of Energy, including at our national labs. We do not yet know how secure the classified systems are at DOE headquarters, but the preliminary reports that I have seen about the testimony we're going to hear today are troubling. It means that Department of Energy has been out looking at all of its contractors and subcontractors, and at the periphery of its organization, being critical, and rightly critical, while it didn't have its own house in order.

General Habiger, you and I were trained in some of the same places, with similar kinds of ethics and values, and I think both of us believe in leadership by example. And I am glad that you're now looking at the Department of Energy headquarters and trying to lead by example. But I am a little sorry that it took this kind of prodding to get the Department of Energy to do so.

With respect to information systems and cyber security and computer security, all of us know that it must be systemic. It is by its nature systemic, and computer security has to be looked at as a whole and not just in pieces. I suspect that is one of the problems at the Department of Energy. Every little fiefdom within the Department of Energy runs its own show, and part of it is weak.

I do want to say something, just briefly, about the reports yesterday from Los Alamos National Laboratory. Folks from Los Alamos came to my office yesterday to give me preliminary information about the loss of classified data at Los Alamos National Laboratory, and I find it deeply troubling. We don't yet know a lot about what happened, and I support the ongoing investigation to find out.

I have also requested that the Intelligence Committee, on which I sit, hold an immediate classified briefing on what was lost and what we know at this point.

There are a number of questions that I still have. They're inappropriate to ask in an unclassified forum, and I will be asking those questions in the House Permanent Select Committee on Intelligence as early as this week.

There is one thing, though, that this most recent incident underscores for me, and that is the need to move forward rapidly with the implementation of the NNSA and the confirmation of General John Gordon to lead it. At the moment, the nuclear weapons complex in this country is in a state of limbo, of neither being part of the Department of Energy nor having a real head of its own. That is unsustainable if we want that organization to move forward, to improve security at our national labs and our nuclear weapons complex, and to come up with a concerted plan for the future.

Thank you, Mr. Chairman.

Mr. UPTON. Thank you. Well, gentlemen, as you know, as you have testified before, we have a long-standing tradition of taking testimony under oath before this subcommittee. Do you have any objection to that?

VOICES. No.

Mr. UPTON. And committee rules allow you to be represented by counsel if you wish such. Do you desire to have counsel representation?

VOICES. No, sir.

Mr. UPTON. In that case, if you would now stand and raise your right hands.

[Witnesses sworn.]

You are now under oath, and as you heard at the beginning, I guess we're going to allow you to take a little extra time in delivering your testimony.

Mr. Podonsky, we'll start with you. Welcome back.

TESTIMONY OF GLENN S. PODONSKY, DIRECTOR, OFFICE OF INDEPENDENT OVERSIGHT AND PERFORMANCE ASSURANCE, ACCOMPANIED BY BRADLEY A. PETERSON, OFFICE OF CYBER SECURITY AND SPECIAL REVIEWS, U.S. DEPARTMENT OF ENERGY

Mr. PODONSKY. Thank you, Mr. Chairman. I appreciate the opportunity to——

Mr. UPTON. If you could just pull the mike a little bit closer, that would be terrific.

Mr. PODONSKY. I appreciate the opportunity, Mr. Chairman, to appear before this committee to discuss our April inspection of unclassified cyber security systems at the DOE headquarters.

As you know, the Office of Independent Oversight and Performance Assurance provides the Secretary of Energy with an independent view of the effectiveness of safeguards and security, emergency management, and cyber security policies and programs throughout the DOE complex. With me this morning is Mr. Brad Peterson, the head of my cyber security office.

In the past, DOE sites often focused on making information easily available and computer systems easy to use, which frequently led to cyber security receiving a low priority. Also, DOE policy was not always followed, which allowed implementation of computer systems in ways that did not provide for effective security.

Particularly disturbing to us was the situation in 1994 at Los Alamos when my office pointed out that the classified network had connections to the unclassified network, posing the risk that an authorized user could download large quantities of classified information to an unclassified computer with little chance of detection.

Over the past 15 years, the DOE headquarters has often received less than satisfactory ratings in many areas, including cyber security. Until Secretary Richardson's involvement, the program offices were in some cases unwilling to commit resources to enhance security. Recent results, however, have been more positive. A number of cyber security upgrades and other initiatives have been completed or are under way.

The results of our inspection in April indicate that important deficiencies still need to be addressed. Many program offices have cyber security programs that would be considered effective if they were not connected to less effective networks.

Generally, the main headquarters fire wall is effective; however, several Web servers managed by individual program offices are located completely outside the fire wall boundary. Most were found to be vulnerable to hacking, and some have vulnerabilities that could allow any Internet user to gain system administrator-level privileges and subsequently deface or shut down the Web site. Headquarters has not developed overall cyber security procedures or minimum requirements for each network segment on the network.

The fragmented management systems and practices currently in place are a root cause of many identified weaknesses. While the chief information officer has attempted to address many of these weaknesses, the effectiveness of these initiatives has been limited due to lack of real or perceived authority. This fragmentation results in part from weaknesses in policy, which does not address the unique situation at headquarters or establish overall responsibilities and authorities.

My office is continually expanding its ability to conduct network performance testing, using tools we have acquired or developed. We currently have an extensive cyber security laboratory dedicated to testing cyber security features. We also conduct regular inspection of cyber security systems at DOE sites.

We will conduct an inspection of the classified cyber security at DOE headquarters next month in conjunction with a comprehensive inspection of all the safeguards and security policies and programs at the headquarters. We also will continue to follow up and work closely with General Habiger's office as they work to clarify and enhance cyber security policy and guidance.

Although much work remains, it is clear that a positive trend in classified cyber security has been established at the headquarters and that DOE headquarters has heard the wake-up call from the Secretary and from the congressional committees. Cyber security is receiving a significantly higher level of attention from senior management than in the years gone past, and we are seeing more improvements that could not have been made without management support and the Secretary's involvement.

Finally, our independent oversight function as a direct report to the Secretary has a mechanism in place, a mandated corrective action plan, that ensures independent oversight findings will be addressed. With these measures, we expect the identified weaknesses will be corrected.

Thank you, Mr. Chairman.

[The prepared statement of Glenn S. Podonsky follows:]

PREPARED STATEMENT OF GLENN S. PODONSKY, DIRECTOR, OFFICE OF INDEPENDENT OVERSIGHT AND PERFORMANCE ASSURANCE, U.S. DEPARTMENT OF ENERGY

Thank you Mr. Chairman. I appreciate the opportunity to appear before this committee to discuss our Independent Oversight activities as they relate to unclassified cyber security at DOE Headquarters. The Office of Independent Oversight and Performance Assurance is responsible for providing the Secretary of Energy with an independent view of the effectiveness of DOE policies and programs in the areas of safeguards and security, emergency management, and cyber security.

My remarks this morning will focus on the recent Independent Oversight inspection of unclassified cyber security systems at the DOE Headquarters, which was conducted in April 2000. I will also briefly summarize some historical perspectives to provide a background on how we got to where we are today. Finally, I will discuss our plans for upcoming inspections at DOE Headquarters, follow-up activities, and other initiatives.

Historical Perspectives.

From the early days of computer networks, DOE has historically struggled with the area of cyber security. For a variety of reasons, such as the emphasis on intellectual freedom and open exchange of ideas, DOE sites, in the past, often focused on making information easily available and computer systems easy to use. This often led to situations in which cyber security received a lower priority than user convenience or operational efficiency.

There were also instances where DOE and contractor management did not follow DOE policy and allowed sites to implement computer systems in ways that did not provide for effective security. A particularly disturbing example was the situation in Los Alamos in 1994 when my office pointed out that the classified network had connections to the unclassified network, which posed a risk from an insider. Using these connections, an authorized user could download large quantities of classified information to an unclassified computer with little chance of detection.

During most Oversight inspections over the last 15 years, the DOE Headquarters has performed poorly, often receiving less than satisfactory ratings in many areas, including cyber security. In many cases, until Secretary Richardson's involvement, Headquarters program offices were unwilling to commit resources to enhance security or to implement the same requirements they imposed on the field.

Recent results, however, have been more positive. Headquarters has completed a number of cyber security upgrades and has other initiatives underway.

Before talking about the results of the recent Headquarters inspection, I would like to take a moment to share with you some of the techniques we use for evaluating the effectiveness of cyber security programs. We began to use automated tools to performance test security features in 1995. This use of technology was a quantum step forward and dramatically increased our ability to test network security. Using automated network scanning tools, we are able to test thousands of systems and all network connections and features in a period of a week. Previously, such an effort would have taken a year or more.

We have continually expanded our ability to conduct performance tests of networks using tools that we have acquired or developed on our own. For example, we have software programs—referred to as "war dialers"—that can test every phone line at a DOE site in a matter of days to determine whether unauthorized modems exist. If present, such modems could be located and used by hackers to bypass the firewall to gain access to information or destroy data.

We currently have an extensive cyber security laboratory dedicated entirely to testing cyber security features. We conduct regular inspections of the implementation of cyber security at DOE sites. We have expanded our methods to include a program of unannounced inspections and penetration testing. Most recently, we have been implementing what is commonly referred to as a RED Team approach, in which we use a variety of techniques to perform detailed tests of a site's cyber security features. These tests include penetration testing by experts who are thoroughly familiar with the latest hacker techniques and methods.

Our assembled team of inspectors, together with our cyber security laboratory, enables us to conduct penetration testing on par with some of the best known hackers. With this extensive testing capability, it is not surprising that we continue to find weaknesses in implementation. Many DOE sites recently have established their own programs for regular scans of their networks and tests of their security features. This is one of the most positive trends in DOE, because an ongoing, effective self-assessment program is essential to effective network security.

In addition to the rigorous performance testing of systems, our inspections also include an evaluation of the programmatic, management system elements that are the essential foundation of a cyber security program. By looking at such elements as leadership, risk management, procedures and performance evaluation, we are able to identify not only specific technical deficiencies, but also underlying root causes, which must be addressed to prevent recurrence of the problems.

Summary of the April inspection of HQ unclassified cyber security systems

The results of our April Headquarters inspection of unclassified cyber security indicate that important deficiencies need to be addressed. Many program offices have cyber security programs that would be considered effective if evaluated on their own merits (that is, they would be effective if they were not connected to less effective networks of other organizations). Within several program offices, leadership and support for cyber security are good, and roles and responsibilities are well defined. Much of the recent improvement can be attributed to the attention and efforts of Secretary of Energy and the DOE Chief Information Officer to improve cyber security across the complex. The Chief Information Officer has been aggressive in creating policy and has taken an active role in addressing DOE-wide problems. The CIO has worked to strengthen cyber security within the Headquarters and improve the security of the network backbone and main firewall. The CIO has also supported the Headquarters program offices through efforts such as regular scanning of networks to identify vulnerabilities that need corrective action.

Despite recent progress, weaknesses continue to exist in several important aspects of the Headquarters cyber security program. Weaknesses regarding the backbone switches and individual systems throughout the network were identified. Our testing demonstrated how a malicious insider could exploit these weaknesses. The results of these tests demonstrate the need for continued vigilance of network security.

Generally, the main Headquarters firewall was effective. However, several Web servers are managed by individual program offices and are located completely outside the firewall boundary. Most of these servers were found to be vulnerable to common hacking exploits, and some contain vulnerabilities that could allow any Internet user to gain system administrator-level privileges, and subsequently deface or shut down the Web site. To demonstrate this possibility, we exploited one of the vulnerabilities and gained system administrator-level privileges to one of the servers. There is also some concern that the risk of alternate pathways into the network that could allow unauthorized access has not been evaluated.

The potentially exploitable vulnerabilities in the Headquarters network result from a number of weaknesses in the unclassified cyber security program. Headquarters has not developed overall cyber security procedures (such as policies for modems or foreign national access) or procedures to establish minimum requirements for each network segment on the network. There is no formal process for evaluating performance and for self-identifying and correcting vulnerabilities in the overall network. Additionally, Headquarters risk assessments have not been rigorous.

The fragmented management systems and practices currently in place are a root cause of many of the programmatic weaknesses and technical vulnerabilities. While the DOE Chief Information Officer has attempted to address many of the weaknesses associated with this fragmentation, we determined that the effectiveness of these initiatives has been limited due to the lack of real and perceived authority. This fragmentation results in part from weaknesses in policy, which does not address the unique situation at DOE Headquarters or establish overall responsibilities and authorities for Headquarters. The 25 individual LAN segments, covering 29 different program offices, have widely varying levels of effectiveness.

While some program offices have established effective practices, others have poor configuration management practices, ineffective policies and procedures, and ineffective intrusion detection strategies. Because of the configuration of the overall network (that is, the logical connections among all systems with few security barriers between segments), the overall system is only as good as the weakest link. In effect, the potentially effective practices of some program offices are largely negated by the ineffective practices of other program offices.

To summarize the results of our inspection, the increased focus on cyber security and the positive measures that have been implemented at DOE Headquarters have resulted in significant improvements in cyber security. However, additional improvements are needed, with particular emphasis on assessing and managing risk and on addressing vulnerabilities that can be exploited from within the internal network.

Plans for Independent Oversight Follow-up and other DOE Initiatives

We will be performing follow-up activities to determine whether identified weaknesses have been addressed. Although in the early stages of their corrective actions.

Headquarters personnel have been generally responsive to the inspection findings and have started corrective actions.

In a related effort, we will be conducting an inspection of the "classified" cyber security program at DOE Headquarters in July 2000 in conjunction with a comprehensive inspection of Headquarters' safeguards and security policies and programs. Independent Oversight will also continue to work with the Office of Security and Emergency Operations as they work to clarify and enhance cyber security policy and guidance.

Although much work remains, it is clear that a positive trend has been established at DOE Headquarters in the area of unclassified cyber security. While continued, close Independent Oversight attention is warranted, there are several reasons to be cautiously optimistic that this positive trend will continue. For example, it is clear that DOE Headquarters has heard the wake-up call from the Secretary and Congressional Committees. Cyber security is receiving a significantly higher level of attention from senior management than in the past, and we are seeing some improvements that could not have been made without management support and the Secretary's personal involvement. In addition, the Office of Security and Emergency Operations and the DOE Chief Information Officer have indicated a willingness to improve policies and guidance to ensure there is a clear and unambiguous basis for holding line management accountable for effective security. Finally, our Independent Oversight function, as a direct report to the Secretary, has a mechanism in place—the mandated corrective action plan—that ensures Independent Oversight findings are addressed. With these measures, we have reason to be optimistic that identified weaknesses will be corrected.

Thank you Mr. Chairman; this concludes my comments.

Mr. UPTON. General Habiger.

TESTIMONY OF EUGENE E. HABIGER, DIRECTOR, OFFICE OF SECURITY AND EMERGENCY OPERATIONS, ACCOMPANIED BY JOHN M. GILLIGAN, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF ENERGY

Mr. HABIGER. Mr. Chairman, distinguished members of this subcommittee, thank you for the opportunity to appear before you today to testify on Mr. Podonsky's Office of Independent Oversight and Performance Assurance report on our headquarters. While not always pleasant to hear, these reviews are essential in our ongoing efforts to ensure that we protect our information systems and the information they process.

I readily acknowledge and accept the findings of this review. As recognized by the review itself, we have made much progress in the headquarters unclassified security program over the past 2 years. The Office of Chief Information Officer, under the very capable leadership of John Gilligan, has moved aggressively to address DOE-wide problems to include the establishment of new policy governing our unclassified systems. At headquarters, John and his staff have made significant improvements in the security of the network backbone and our main firewall. Despite this progress, however, I acknowledge there is room for improvement.

I also want to be straightforward with you and freely admit that over the past year our focus has been directed at our defense facilities and then our other large sites. As a result, headquarters has not received the same level of attention. This level of attention is directly correlated to the funds appropriated to us for cyber security. As part of our fiscal year 2000 Budget Amendment Request that I was personally involved with in July of last year, we asked for $35 million to address our cyber security needs, but were appropriated only $7 million. With such a shortfall, some hard decisions had to be made.

Mr. Chairman, I now quote from my sworn testimony of October 26 of last year in front of this very committee, "Congress has, up to this point, failed to fund the Department's fiscal year 2000 full budget amendment in order for us to make near- and long-term fixes. We have valid requirements in the area of cyber security to buy hardware, encryption equipment and to train our systems administrators. Simply stated, we have been given a mandate, but not the resources to accomplish that mandate."

I cannot in retrospect tell you that if we had received the additional $28 million we requested back in July that we would have no cyber security discrepancies, but I can assure you, Mr. Chairman, that in my judgment they would not have been of the same order of magnitude.

Consequently, the headquarters unclassified cyber security initiatives were given lower priority in light of more pressing needs at our field sites. Granted, not all of the issues identified were the result of funding shortfalls. Where limited funds were not an issue, we moved quickly to take corrective action.

In addition, the Deputy Secretary recently directed that the Office of Chief Information Officer serve as the central cyber security authority for the headquarters. This action addresses the recommendations to establish the necessary management structure to implement an effective cyber security program at our headquarters.

Additionally, we are implementing longer-term actions to improve the efficiency of the cyber security program by adopting best security practices and a more proactive risk assessment program.

I want to assure you that we are fixing the shortfalls identified in the independent oversight review. Headquarters should and will set the standard for the rest of the Department on how it implements security of our unclassified systems.

Thank you, Mr. Chairman.

[The prepared statement of Eugene E. Habiger follows:]

PREPARED STATEMENT OF EUGENE E. HABIGER, DIRECTOR, OFFICE OF SECURITY AND EMERGENCY OPERATIONS, U.S. DEPARTMENT OF ENERGY

Mr. Chairman and distinguished members of the Subcommittee, thank you for the opportunity to appear before you today to testify on the Office of Independent Oversight and Performance Assurance's report entitled, "Unclassified Cyber Security Review of Department of Energy Headquarters." While not always pleasant to hear, these reviews are essential in our ongoing efforts to ensure that we protect our information systems and the information that they process.

I readily acknowledge and accept the findings of the Independent Oversight review. As recognized by the review itself, we have made much progress in the Headquarters unclassified cyber security program over the past two years. The Office of the Chief Information Officer, under the very capable leadership of John Gilligan, has moved aggressively to address DOE-wide problems to include the establishment of new policy governing our unclassified systems. At Headquarters, John and his staff have made significant improvements in the security of the network backbone and main firewall. Despite this progress, however, there is room for improvement.

I also want to be straightforward with you and freely admit that over the past year our focus has been directed at our defense facilities and then our other large sites. This level of attention is directly correlated to the funds appropriated to us for cyber security. As part of our FY 2000 Supplemental Budget Amendment request, we asked for $35 million to address our cyber security needs, but were appropriated only $7 million. With such a shortfall, some hard decisions had to be made.

Mr. Chairman, I now quote from my sworn testimony of October 26, 1999 in front of this committee: "... Congress has, up to this point, failed to fund the Department's FY 2000 full budget amendment in order to make near and long term fixes. We have valid requirements in the area of cyber security to buy hardware, encryption equipment and to train our systems administrators ... Simply stated, we have been given a mandate but not the additional resources to accomplish that mandate." I cannot in retrospect tell you that had we received the additional $28M we requested back in July of last year, that we would have had no cyber security discrepancies ... but, I can assure you that they would not have been of the same order of magnitude.

Consequently, the Headquarters unclassified cyber security initiatives were given lower priority in light of more pressing needs at our field sites. Granted, not all of the issues identified were the result of funding shortfalls. Where limited funds were not an issue, we moved quickly to take corrective action. For example, the Deputy Secretary recently directed that the Office of the Chief Information Officer serve as the central cyber-security authority for Headquarters. This action addresses the recommendation to establish the necessary management structure to implement an effective cyber-security program at Headquarters.

Additionally, we are implementing longer-term actions to improve the efficiency of the cyber security program by adopting

- best security practices, and
- a more proactive risk assessment program.

I want to assure you that we are fixing the shortfalls identified in the Independent Oversight review. Headquarters should and will set the standard for the rest of the Department on how it implements security of its unclassified systems. With your permission, I would now like to yield to John Gilligan, the Chief Information Officer of the Department of Energy, to elaborate on how we are progressing on our Headquarters efforts.

Mr. UPTON. Mr. Gilligan.

TESTIMONY OF JOHN M. GILLIGAN

Mr. GILLIGAN. Thank you, Mr. Chairman and distinguished members of the subcommittee, for the opportunity to appear before you today. My testimony will focus on actions we have taken across the Department to improve the level of cyber security protection in our systems and networks. I will also discuss the cyber security weaknesses that have been identified in the headquarters during the recent review by the Department's independent oversight organization, as well as our efforts to remedy these identified weaknesses.

I am pleased to say that the state of cyber security at the Department of Energy is far better today than it was a year ago. A year ago there was clear evidence that the Department's cyber security efforts, in particular for our unclassified computer systems, had not kept pace with the rapid proliferation of network connection and increasing threats. Our policies were outdated, cyber security compromises at some sites led to significant work disruptions, and we did not have awareness of cyber security threats or adequate training of our work force to deal with these threats. These concerns were reported in congressional hearings and other forums. This was a painful wake-up call for the Department, but a necessary one.

During the past year, each DOE organization has focused on improving awareness of cyber security threats and installing improved security controls. I have seen enormous progress in how unclassified information is protected and a significant increase in the awareness of cyber security issues at all levels within the Department. While we have worked this issue aggressively, cyber security is not a quick fix and more needs to be done. However, the security protection in the Department is improving rapidly, and I appreciate the opportunity to discuss our progress.

Since the spring of 1999, the Secretary of Energy and I have emphasized the Department-wide focus on cyber security. The initial focus was on our defense laboratories and production facilities, with aggressive programs to upgrade and verify fixes at these facilities last summer and fall. This focus has subsequently been extended to all DOE sites. Over this period, the Department has completely restructured its cyber security program. Actions taken include the following:

Creating a single Department-wide cyber security office under me as the Department's Chief Information Officer; requiring work stand-downs at all sites to conduct security awareness training; developing and issuing four new cyber security policies and two new cyber security guidelines; instituting a set of cyber security metrics which permit us to evaluate progress at each site; doubling the size and increasing the role of the central DOE security incident and early warning capability, our computer incident advisory capability located at Lawrence Livermore Laboratory; having each DOE site develop a detailed site-specific cyber security plan describing the implementation of cyber security protection at the site; deploying a number of security training programs Department wide to improve the security skills of our systems administrators and a separate training course provided to our line managers.

Finally, each site has significantly upgraded its protection through the use of firewalls and intrusion detection software, stronger passwords, improved system configuration controls and reconfiguration of system and network connectivity to reduce vulnerabilities.

In addition, the Secretary has created a proactive, independent security assessment organization, the Office of Independent Oversight and Performance Evaluation, reporting directly to him, to provide an independent review of security throughout the complex. For the past year, this independent oversight office has been conducting thorough reviews of cyber security effectiveness at DOE sites.

As Chief Information Officer, I am a key customer of the products of the independent oversight reviews. I rely on these reviews to provide me with an objective assessment of the effectiveness of the cyber security at our sites and the effectiveness of the CIO cyber security policies. In essence, the independent oversight reviews provide critical feedback to me on how the individual sites are progressing with cyber security upgrades, and my staff often participates in the reviews.

Since last summer the independent oversight organization has conducted 13 reviews. In those instances where significant vulnerabilities were identified, my policy staff and I have worked with the site and the line management organizations to ensure that there is rapid resolution. Action plans for fixing problems identified in the independent oversight reviews are tracked by the DOE Security Council that is chaired by the DOE Security Czar General Habiger.

In cases where there are significant weaknesses identified, a rapid follow-up review by the independent oversight team is scheduled. We have done such follow-up reviews at a number of our facilities over the past year. These follow-up reviews provide me and other senior Department officials with clear evidence that those sites are, in fact, making rapid progress to remedy the identified cyber security problems.

In April of this year, the DOE independent oversight office conducted a review of the headquarters unclassified cyber security program. This assessment included a programmatic review and testing of controls to prevent or limit access to the headquarters information network against the external threats, such as unauthorized system hackers, and internal threat, for example, Department employees.

As you have heard from Mr. Podonsky, the review found that, although unclassified cyber security at headquarters has significantly improved in the past 2 years, there are still significant deficiencies that need to be addressed. In particular, the review found that many program offices within the headquarters have effective cyber security programs. However, because all DOE headquarters networks are interconnected, an office with weak security can undermine the otherwise effective processes and controls of the better managed offices. A number of individual headquarters offices were found to have ineffective cyber security programs.

Weaknesses identified in the review included the following: A lack of headquarters-wide procedures on configuration management; the absence of consistent policy on external connections, modems and foreign national access; the lack of minimum cyber security requirements for each local area network in the headquarters; lack of a formal process to evaluate performance and self-identify and correct cyber security vulnerabilities; headquarters risks assessments had also not been done rigorously and had not considered the shared risks of the headquarters network.

In my assessment, the root cause for most of the reported cyber security problems was the failure to treat the headquarters as an interconnected and interdependent set of systems and network, that is, an integrated site. This problem started to become apparent earlier this spring when I found that each office in the headquarters had produced separate cyber security plans as required by DOE's new unclassified cyber security policy. The reviews by my office of many of these plans indicated serious weaknesses. These were documented and forwarded back to the individual organizations.

In addition, as we began to collect metrics on cyber security implementation, the metrics submitted from some headquarters offices indicated that they had significant weaknesses in their cyber security implementation programs. These findings were shared with the respective headquarters management, and we began evaluating approaches to improve our approach within the headquarters. The findings of the independent oversight review confirmed these earlier indications of problems.

The Office of Independent Oversight has recommended immediate and long-term actions to address the headquarters cyber security issues identified in its review. I support these recommendations. Immediate actions include designating a single focal point for headquarters cyber security as well as establishing appropriate processes and procedures across the headquarters. Longer-term actions include taking steps to improve the efficiency of cyber security programs by adopting best security practices and a more proactive risk management program.

Steps that are being taken to address the recommendations made by the Office of Independent Oversight are as follows: On June 8, the deputy-secretary directed the Office of the CIO to serve as central cyber security authority for all computers and networks within the Department of Energy headquarters site, and I have submitted that memorandum as a part of the testimony. This action is the necessary and important first step to begin to manage headquarters as a single entity and to institute consistent site-wide approaches for securing our computers and networks.

Specifically, the CIO operations organization, headed by Mr. Patrick Hargett who has joined me, which currently provides computer and networking support to a number of headquarters organizations, including the Office of the Secretary, the CIO, Security and Emergency Operations, Management and Administration, the Chief Financial Officer and a number of other offices, will assume responsibility for all cyber security policies, processes and procedures for the entire headquarters site. These policies, processes and procedures will be coordinated through a headquarters cyber security working group that my office will form. Each headquarters office will also be represented on this working group and will be an integral part of the cyber security forum.

In addition, my office, as the central cyber security authority for headquarters, will undertake the following efforts: develop, implement and enforce formal network connection policies; develop, manage, operate and enforce an integrated security configuration management process; develop, manage and implement a security self-assessment process for headquarters offices; and centrally manage the security of headquarters, the network perimeter, including all firewalls and be responsible for performing intrusion detection, vulnerability scanning and auditing on the headquarters information technology infrastructure.

I have made a commitment to the Secretary that we will implement fixes to the significant vulnerabilities identified in the independent oversight review of the headquarters within 60 days. Consistent with our practices when we find a site that has significant weaknesses, I have asked the Office of Independent Oversight to reassess the headquarters in early fall to verify that we have resolved the serious weaknesses that were identified in the April review. The Secretary has requested regular updates on progress to close the headquarters vulnerabilities.

In summary, the cyber security program in the Department of Energy in June 2000 bears little resemblance to the program in place just a year ago. We have put updated cyber security policies in effect, our security training has improved the effectiveness of our system administrators and informed our management of upgraded cyber security threats, each site has upgraded its security controls and have improvement plans to be executed as resources are available, and a review and follow-up process using the Secretary's independent oversight function permits the Department to objectively assess our status.

Although we have made great process, there is room for improvements. Clearly, the review of the headquarters shows that we have significant weaknesses that require immediate attention. Moreover, the Department believes that the headquarters must set the standard for the rest of the Department on how it implements security of its cyber systems. The Secretary and I are fully committed to ensuring that the headquarters is a model for the rest of the Department.

Beyond fixing the clear weaknesses, the Department is moving to strengthen security in a number of areas. Current focus areas for improvement are eliminating the use of clear text reusable passwords, implementing consistent security architectures at each site, using automated tools to review firewall and intrusion detection logs to identify and then automatically block access from Internet sites that are attacking DOE sites, and automated distribution of software patches to make the process of patching vulnerabilities more rapid and reliable.

We know that there is no silver bullet fix for cyber security. Success in this area will take continued focused efforts to deal with the increasing complexity of the threats and the rapid evolution of technology.

Successes will also take resources. I note that as a part of the Department's fiscal year 2000 Budget Amendment request, we asked for additional funding to address our pressing security needs for our unclassified computers, but, as General Habiger noted, we were only appropriated a small portion of what was requested.

While many of the issues identified in the review of the headquarters and other DOE sites are not the result of lack of funding, accelerating implementation of protection mechanisms does take additional resources.

We look forward to continuing to work with the Congress to fund our important cyber security programs, and we commit to providing you continued visibility on our progress. Thank you.

[The prepared statement of John M. Gilligan follows:]

PREPARED STATEMENT OF JOHN M. GILLIGAN, CHIEF INFORMATION OFFICER, U.S. DEPARTMENT OF ENERGY

INTRODUCTION

Thank you Mr. Chairman and distinguished members of the Committee for the opportunity to appear before you today. My testimony will focus on actions we have taken across the Department to improve the level of cyber security protection in our systems and networks. I will also discuss the cyber security weaknesses that have been identified in the Headquarters during the recent review by the Department's Independent Oversight organizations, as well as our efforts to remedy these identified weaknesses.

I am pleased to say that the state of cyber security at the Department of Energy (DOE) is far better today than it was a year ago. A year ago, there was clear evidence that the Department's cyber security efforts, in particular for our unclassified computer systems, had not kept pace with the rapid proliferation of network connections and increasing threats. Our policies were outdated, cyber security compromises at some sites led to significant work disruptions, and we did not have awareness of cyber security threats or adequate training of our workforce to deal with these threats. These concerns were reported in congressional hearings and other forums. This was a painful wake-up call for the Department, but a necessary one.

During the past year, each DOE organization has focused on improving awareness of cyber security threats and installing improved security controls. I have seen enormous progress in how unclassified information is protected and a significant increase in awareness of cyber security issues at all levels within the Department. While we have worked this issue aggressively, cyber security is not a quick fix and more needs to be done. However, the security protection in the Department is improving rapidly, and I appreciate the opportunity to discuss our progress.

Since the spring of 1999, the Secretary of Energy and I have emphasized a Department-wide focus on cyber security. The initial focus was on our Defense laboratories and production facilities with aggressive programs to upgrade and verify fixes at these facilities last summer and fall. This focus has subsequently been extended to all DOE sites. Over this period, the Department completely restructured its cyber security program. Actions taken include the following:

- Creating a single, Department-wide Cyber Security Office under me as the Department's Chief Information Officer.
- Requiring work "stand downs" at all sites to conduct security awareness training.
- Developing and issuing four new cyber security policies and two new cyber security guidelines.
- Instituting a set of cyber security metrics which permit us to evaluate progress at each site.
- Doubling the size and increasing the role of the central DOE security incident and early warning capability, our Computer Incident Advisory Capability (CIAC) located at Lawrence Livermore Laboratory.
- Having each DOE site develop a detailed, site-specific cyber security plan describing the implementation of cyber security protection at the site.
- Deploying a cyber security training program Department-wide to improve the security skills of our Systems Administrators and a separate training course provided to line managers.
- Finally, each site has significantly upgraded its protection through the use of firewalls and intrusion detection software, stronger passwords, improved system configuration controls, and reconfiguration of system and network connectivity to reduce vulnerabilities.

In addition, the Secretary created a proactive independent security assessment organization, the Office of Independent Oversight and Performance Evaluation, reporting directly to him to provide an independent review of security throughout the complex. For the past year, this Independent Oversight office has been conducting thorough reviews of cyber security effectiveness at DOE sites. As CIO, I am a key customer of the products of independent oversight reviews. I rely on these reviews to provide me with an objective assessment of the effectiveness of the cyber security at our sites and the effectiveness of the CIO cyber security policies. In essence, the Independent Oversight reviews provide critical feedback to me on how individual sites are progressing with cyber security upgrades, and my staff often participates in the reviews. Since last summer, the Independent Oversight organization has conducted 13 reviews. In those instances where significant vulnerabilities were identified, my policy staff and I have worked with the site and the line management organization to ensure that there is rapid resolution. Action plans for fixing problems identified in the Independent Oversight Reviews are tracked by the DOE Security Council that is chaired by the DOE Security Czar, General Habiger. In cases where there are significant weaknesses identified, a rapid follow-up review by the Independent Oversight team is scheduled. We have done such follow-up reviews at a number of our facilities over the past year. These follow-up reviews provide me and other senior Department officials with clear evidence that those sites are, in fact , making rapid progress to remedy the identified cyber security problems.

INDEPENDENT OVERSIGHT REVIEW

In April of this year, the DOE Independent Oversight office conducted a review of the Headquarters unclassified cyber security program. The assessment included a programmatic review and testing of controls to prevent or limit access to the Headquarters information network against the external threat (such as unauthorized system, i.e., hackers) and the internal threat (i.e., Department employees). As you have heard from Mr. Podonsky, the review found that, although unclassified cyber security at Headquarters has significantly improved in the past two years, there are significant deficiencies that need to be addressed. In particular, the review found that many program offices within the Headquarters have effective cyber security programs. However, because all DOE Headquarters networks are interconnected, an office with weak security can undermine the otherwise effective processes and controls of the better-managed offices. A number of individual Headquarters offices were found to have ineffective cyber security programs.

Weaknesses identified in the review included the following:

- A lack of Headquarters-wide procedures on configuration management;
- The absence of consistent policy on external connections, modems, and foreign national access;
- The lack of minimum cyber security requirements for each Local Area Network in the Headquarters;
- Lack of a formal process to evaluate performance and self-identify and correct cyber security vulnerabilities;
- Headquarters risk assessments had not been rigorous and had not considered the shared risk of the Headquarters network.

In my assessment the root cause for most of the reported cyber security problems was the failure to treat the Headquarters as an interconnected and interdependent set of systems and networks that is an integrated "site". This problem started to become apparent earlier this spring when I found that each office in the Headquarters had produced separate cyber security plans as required by DOE's new unclassified cyber security policy. The reviews by my office of many of these plans indicated serious weaknesses. These were documented and forwarded back to the individual organizations. In addition, as we began to collect metrics on cyber security implementation, the metrics submitted from some Headquarters offices indicated that they had significant weaknesses in their cyber security programs. These findings were shared with the respective Headquarters management, and we began evaluating approaches to improve our approach within the Headquarters. The findings of the Independent Oversight review confirmed these earlier indications of problems.

The Office of Independent Oversight has recommended immediate and long-term actions to address the headquarters cyber issues identified in its review. I support these recommendations. Immediate actions included designating a single focal point for Headquarters Cyber Security, as well as establishing appropriate processes and procedures across Headquarters. Longer-term actions include taking steps to improve the efficiency of the cyber security program by adopting best practice security practices and a more proactive risk assessment program.

DEPARTMENT RESPONSE TO INDEPENDENT OVERSIGHT REPORT

Steps that are being taken to address the recommendations made by the Office of Independent Oversight are as follows. On June 8, 2000, the Deputy Secretary directed the Office of the CIO to serve as the central cyber security authority for all computers and networks within the DOE Headquarters site (see attachment). This action is the necessary and important first step to begin to manage Headquarters as a single entity and to institute consistent site-wide approaches for securing our computers and networks. Specifically, the CIO Operations Organization, which currently provides computer and networking support to a number of Headquarters organizations including the Office of the Secretary, the CIO, Security and Emergency Operations,

Management and Administration, the CFO and a number of other offices, will assume responsibility for all cyber security policies, processes, and procedures for the entire Headquarters site. These policies, processes and procedures will be coordinated through a Headquarters Cyber Security Working Group that my office will form. Each Headquarters office will be represented on this Working Group and will be an integral part of this cyber security forum.

In addition, my office, as the central cyber security authority for the Headquarters, will undertake the following efforts:

- Develop, implement and enforce formal network connection policies;
- Develop, manage, enforce and operate an integrated security configuration management process;
- Develop, manage and implement a security self-assessment process for Headquarters offices; and
- Centrally manage the security of the Headquarters network perimeter, including all firewalls, and be responsible for performing intrusion detection, vulnerability scanning and auditing on the Headquarters IT infrastructure.

I have made a commitment to the Secretary that we will implement fixes to the significant vulnerabilities identified in the Independent Oversight review of the Headquarters within sixty days. Consistent with our practices when we find a site that has significant weaknesses, I have asked the Office of Independent Oversight to reassess the Headquarters in early fall to verify that we have resolved the serious weaknesses that were identified in the April review. The Secretary has requested regular updates on progress to close the Headquarters vulnerabilities.

CONCLUSION

In summary, the cyber security program in the Department of Energy in June of 2000 bears little resemblance to the program in place just a year ago. We have put updated cyber security policies in effect; our security training has improved the effectiveness of our system administrators and informed our management of upgraded cyber security threats; each site has upgraded its security controls and have improvement plans to be executed as resources are available; and a review and follow-up process using the Secretary's Independent Oversight function permits the Department to objectively assess our status. Although we have made great progress, there is room for improvements. Clearly, the review of the Headquarters shows that we have significant weaknesses that require immediate attention. Moreover, the Department believes that the Headquarters must set the standard for the rest of the Department on how it implements security of cyber systems. The Secretary and I are fully committed to ensuring that the Headquarters is a model for the rest of the Department.

Beyond fixing the clear weaknesses, the Department is moving to strengthen security in a number of areas. Current focus areas for improvement are eliminating the use of clear-text reusable passwords, implementing consistent security architectures at each site, using automated tools to review firewall and intrusion detection logs to identify and then automatically block access from internet sites that are attacking DOE sites, and automated distribution of software patches to make the process of patching vulnerabilities more rapid and reliable.

We know that there is no silver bullet fix for cyber security. Success in this area will take continued and focused effort to deal with the increasing complexity of the threats and the rapid evolution of technology. Success will also take resources. I note that as a part of the Department's FY 2000 Supplemental request, we asked for additional funding to address our pressing security needs for our unclassified computers, but as General Habiger noted, we were only appropriated a small portion of what we requested. While many of the issues identified in the review of the Headquarters and other DOE sites are not the result of lack of funding, accelerating implementation of protections mechanisms does take additional resources. We look forward to continuing to work with Congress to fund our important cyber security programs and we commit to providing you continued visibility on our progress.

Thank You.

Mr. UPTON. Thank you.

I would just note that the House was in session and voting until nearly midnight last night. We also have a number of subcommittees that are also meeting at this time, and by unanimous consent I will ask that all members of the subcommittee will have an opportunity to enter their opening statement into the record.

You will see a number of members coming in and out. We're going into session, I know, at 10. I don't expect votes for a while as we complete yet another long day today on the Labor, HHS appropriation bill.

General Habiger, I know that you're prepared for some of the questions that we're going to have in light of the opening statement by Mr. Bliley, Mr. Stupak and myself with regard to the missing disks and the hard drives; and I happen to find it, as I read the morning papers this morning, fairly incredulous that it appears as though these disks have been missing for a number of weeks. Only 86 individuals had access to these disks, in fact; and, of those 86, only I believe 26 were allowed to have unescorted access to the disks.

A number of members of this subcommittee traveled to look at all the labs earlier this year. We visited extensively, I thought, Los Alamos. We had a number of meetings with your staff and others before we came, terrific staff support as well.

Could you describe the vault? And I don't know that we visited this particular vault where these were taken.

At Los Alamos, the vault we did visit, we went through this long drive through these almost mountain passes and went through security that was very well armed and photo ID. I mean, it was extensive to get in. In fact, I think it took us about 20 minutes to actually get into the vault because of the security. We probably spent more time going through the security to get into the vault than we actually spent in the vault. And I don't know whether that was the vault—you know the groundwork much better because you have been there, I'm sure, a number of times. Is that the vault, the one that actually goes into almost into the mountain where these two disks were taken?

Mr. HABIGER. No, sir. The vault in question is in the main building, technical area three, they call it.

Mr. UPTON. Is that where Wen Ho Lee's office is?

Mr. HABIGER. Yes, sir.

There are three levels of protection before you get into the vault itself. I'd rather not go into the details in open session, but let me tell you that there are extensive security procedures that are in place at each level of in-depth security that would preclude anyone except those that are authorized to be in that area to gain access to the vault. The vault itself serves about—is relatively small, about 10 feet wide and about 20 foot long.

Mr. UPTON. Now, as I understand it, these two disks——

Mr. HABIGER. Two hard drives.

Mr. UPTON. Two hard drives that are missing were, in fact, in a locked bag, is that right, inside the vault?

Mr. HABIGER. Yes, sir.

Mr. UPTON. And in fact, the bag itself was, in fact, compartmentalized, with locked compartments within the bag; is that right?

Mr. HABIGER. Yes, sir.

Mr. UPTON. The way that I understand it is, when it was discovered, the empty compartment was, in fact, locked; is that right?

Mr. HABIGER. Yes, sir.

Let me just back up a little bit and explain the scenario.

The fire at Los Alamos began on, as I recall, Thursday, May 4. On the evening of May 7, Sunday, late, nearly midnight, the decision was made to go into the vault by two individuals who are authorized unescorted access into that vault to take the kit—the kit is a kit used by the Nuclear Emergency Search Team, NEST, to rapidly deploy to situations that require some of our Nation's best minds to look at an improvised nuclear device or perhaps a stolen nuclear weapon. These individuals pull on-call duty. We have members of our scientific community at both Los Alamos, Livermore and Pantex on duty, on call 24 hours a day, 365 days a year.

In order to ensure that that capability was still available to respond very rapidly, the decision was made to go into the vault late Sunday night as the fire began to burn out of control. They went into the vault, they inventoried—and you can inventory the hard drives by just feeling them. They're a little bigger than a deck of cards, about two-thirds as wide as a deck of cards. They could not feel the hard drives in the locked container.

There are three kits. They were in kit No. 2. They immediately went into kit No. 3 to pull out two hard drives. One's the primary. The second hard drive is the backup. They took the two hard drives, the two containers out of kit three, put it in kit two and immediately evacuated the area and put the kit two with the kit three hard drives in a more secure—by secure I'm talking about safe, out of harm's way in relation to the fire.

They immediately reported to other individuals on the NEST team that they went into the vault, they couldn't find the hard drives to kit two, and, as you recall, on Monday, May 8, the lab was shut down completely because of the life-threatening aspects of the fire. The lab did not come back up until Monday, May 22; and when the labs started back up again on Monday, May 22, it was not all 10,000 people going back to work. It was a gradual buildup of activity. The first things that were looked at were the safety considerations.

I will also tell you that during this entire course of the fire, I was in contact—along with Deputy Secretary Glauthier, we had people on duty 24 hours a day, and the security systems were up and running the entire time. Now there were certain situations where we had to pull guards out of certain areas and put them out of harm's way, but we still had a credible security at all of the facilities there, to include this vault.

So the labs started up on Monday, May 22. On Wednesday, May 24, a full-scale search was begun within the X division and anyplace that the NEST activity could have taken place. We were informed on the evening of June 1 that those hard drives were missing.

Ed Curran, the Director of Counter Intelligence, immediately went to the FBI headquarters and informed them. Deputy Secretary Glauthier was in communication with Dr. Browne at the laboratory. On Monday, during a video teleconference with Dr. Browne, it was determined that Dr. Browne indicated that he had intensely searched the facility and could not find the two missing hard drives.

At that point, Deputy Secretary Glauthier directed that I, with Ed Curran, go to FBI headquarters, which we did. We met at around noon with senior officials at the Bureau. It was determined that we jointly do an investigation, DOE and the FBI. At 8:30 that night, Monday night, I was in Los Alamos. At 7 o'clock the next morning, we had a sizable number of FBI agents, about 15, 10 DOE personnel; and we started at 7 o'clock Tuesday morning; and we didn't finish up until nearly midnight that night. Our first interviews began that first day.

I was recalled—I was actively engaged until this past Saturday. I was asked to come back to testify at this hearing. I came back Sunday, and I plan on going back tomorrow.

Mr. UPTON. When you say that there was an intensive search for these disks, was there an intensive search between May 8 and May 22?

Mr. HABIGER. No, sir, because the lab was completely shut down. And you had to be there—and I went there—I went there on May 19, as I recall. I flew over the site; and I will tell you, sir, that it was life threatening. There was absolutely no activity except security and fire fighting that went on from that period—essentially from May 7 through May 22.

Mr. UPTON. But the individuals that had access to the disks, 26 folks who had unescorted access, they weren't then at the facility, right? They all left?

Mr. HABIGER. Yes, sir. Yes, sir. And there's no indication whatsoever—see, there's a log that is created based upon the entry procedures, again which I'd rather not go into here. A telephone call has to be made. That call is recorded. Passwords have to be given. It's an elaborate process.

Mr. UPTON. Right. But was any effort taken with the 26 people that had access to that until the May 22? I mean, what I'm saying is those people weren't there, those 26 people. They went someplace where it was safe. You knew that the disks were missing since May 8. The lab was closed from May 8 to May 22. Those individuals who had access and actually could have perhaps retrieved or taken those disks went someplace where it was safe. Was any effort taken by the Los Alamos security folks to, in fact, interview any of those 26 people during the fire?

Mr. HABIGER. No, sir. The total focus during that period was the—saving the laboratory from destruction from the fire.

Mr. UPTON. But we knew that disks were missing before the fire took place.

Mr. HABIGER. Sir, there were a relatively small number of individuals that knew that. You will have to talk to lab personnel—and, again, we are trying to determine through a series of interviews, the FBI and Department of Energy—at last count over 90 interviews had been accomplished, interviews that last anywhere from 30 minutes to 3 hours since Tuesday of last week. Those interviews continue as we speak.

Mr. UPTON. Are polygraphs being used on those interviews?

Mr. HABIGER. They will be beginning tomorrow, yes, sir.

Mr. UPTON. Mr. Stupak.

Mr. STUPAK. Thank you, Mr. Chairman.

General, you speak of kit No. 2 as having the missing hard drives. Is there a kit No. 1?

Mr. HABIGER. Yes, sir.

Mr. STUPAK. Is that all intact?

Mr. HABIGER. Yes, sir.

Mr. STUPAK. Okay. So the one we're talking about is kit No. 2?

Mr. HABIGER. Absolutely.

Mr. STUPAK. Once you get into the area where the kits are stored, where this NEST kit is stored, aren't the keys to get into these bags just hanging right there on the wall?

Mr. HABIGER. Sir, there are two sets of keys. There's a set of keys on the wall, and there's a set of keys attached to the kit.

Mr. STUPAK. So once you get to the kit area you can have access to those kits either by taking the keys off the wall or ones on the kit; is that right?

Mr. HABIGER. Yes, sir.

Mr. STUPAK. And the people who are in there, there are 26 who had to be escorted and about 60 others who did not need to be escorted?

Mr. HABIGER. Fifty-seven. Sixty's close enough.

Mr. STUPAK. So then when the kit—when it was discovered that kit No. 2 was missing the hard drives and you had the fire, there was no attempt to ascertain from these possibly 56, 57 people and the other 26 people what they did with it during this time?

Mr. HABIGER. Sir, the access to the vault is, as I mentioned, very tightly controlled. Anyone who goes into the vault during off-duty hours has to go through this elaborate procedure to get into the vault where it's documented. There is also a log in the vault for those people who are not allowed unescorted access, that they have to sign in. So those 57 individuals, whenever they went in, they'd have to sign in on a log. They couldn't go in by themselves. I went—when I went to the vault, had to sign in on a log, and I was escorted.

Mr. STUPAK. And hopefully everyone signed in, but we don't know if everyone signed in.

Second, you mentioned off duty. What about regular business hours? Do people sign in all the time then?

Mr. HABIGER. Let me back up, sir. Those kinds of questions are being asked now. I have seen the logs. I can't confirm——

Mr. STUPAK. They may be asked now, but I guess the part that still puzzles me, why weren't they asked between May 8 and May 24 when the fire got under control? Why did it take almost 2 weeks before anyone started asking the questions? These 56 people or 26 people weren't out fighting the fire, were they? Certainly you had access to them. They could have asked these questions.

I would think on May 8 when you're missing the kits, two hard drives from these computers, there'd be some concern and start asking questions. While you have the fire, I'm sure you're not out there fighting the fire. I'm sure someone would have at least started some investigation instead of waiting until June 1 to notify the FBI that everyone's returned, we still can't find these things. I guess that is the laissez-faire attitude that I really have problems with.

Mr. HABIGER. Well, sir, these kinds of questions that you're asking are good questions. And as a result of the investigation, which, by the way, is a criminal investigation at this point, we will find the answers to these questions; and we will take the appropriate action. The lab director will take the appropriate action.

Mr. STUPAK. In the Washington Post this morning you said, and if I can quote you, the disks and the hard drives missing at Los

Alamos were probably misplaced or lost rather than stolen. How did you reach that conclusion?

Mr. HABIGER. Sir, I'd rather not go into that in this session.

Mr. STUPAK. Well, you know, you talked to the Post about it. That is certainly in open session.

Mr. HABIGER. Yes, sir. I will stand by that statement based upon——

Mr. STUPAK. Was that the official line or do you have something to back it up? Is the official line that, well, it must be misplaced or lost rather than stolen or do you really have some proof, without getting into it, that they were, in fact, misplaced?

Mr. HABIGER. It's my judgment, sir, based upon my exposure over the past week of working nearly 15, 16 hours a day and being an integral part of the process.

Mr. STUPAK. Okay. Has anyone yet told you or anyone else that the disks were set down or misplaced and just can't remember where they were? Do you have any idea who was the last person who had access to this kit No. 2?

Mr. HABIGER. Sir, there's no requirement to inventory the disks. As a matter of fact, because of changes in security policies across the entire government, there's very little requirement to inventory classified material.

Mr. STUPAK. So if I get in the vault, I take kit No. 2, I don't have to sign out—don't have to sign it out or anything?

Mr. HABIGER. No, sir.

Mr. STUPAK. So my library book in Menominee is more secure than these disks once I get access, get my hands on it?

Mr. HABIGER. Sir, the individuals who have access to those kits are dedicated, loyal Americans.

Mr. STUPAK. I don't dispute that, but you can't dispute we have two of them missing.

Mr. HABIGER. Yes, sir.

Mr. STUPAK. You can't dispute that when they took them out there's no procedure in place to identify even who took them out. Once you get to the magic ring, you take the magic ring and you leave, and there's no check-out of that.

Mr. HABIGER. But you have to get to the magic ring.

Mr. STUPAK. Right. It sounds like it wasn't too difficult, if you have about 80 or 90——

Mr. HABIGER. There are 26 people who had access, uncontrolled access, unescorted access.

Mr. STUPAK. Okay—26 unescorted access, and then another 56 or 57 who would have to be escorted. And I guess our concern is, if it's 26 who have unescorted and if they're missing the—May 7 or May 8 and they come back May 24, because they were good people, no one thought it was necessary to check with those 26 what happened in the interim?

Mr. HABIGER. No, sir. I think it was a focus on a catastrophic event that was occurring, that many people's lives were at risk.

Mr. STUPAK. I don't disagree with that, but do you think it was a mistake not to at least begin an investigation to try to figure out where they were, if someone honestly misplaced them we could get them back here, so you wouldn't be back here answering my questions?

Mr. HABIGER. Sir, that is one of my questions that we'll have answered as a result of our investigation.

Mr. STUPAK. General, last May, Secretary Richardson said there was a, "zero tolerance security policy." He said, "no security infractions are acceptable, and penalties would be strengthened." These would include, "verified unintentional or reckless breaches that create a significant risk of a national security compromise or that displays a wilful disregard for security procedures." That was May 11, 1999. Is that policy still in place today?

Mr. HABIGER. It certainly is, sir.

Mr. STUPAK. Is what happened at Los Alamos with kit No. 2 a security infraction or is it an oversight by a scientist? At a minimum, you would have to agree the information has left its proper secured location, has it not?

Mr. HABIGER. Sir, I will tell you that when we find the answer to the question as to who was responsible, I guarantee you that that individual will be dealt with appropriately under the Secretary's very aggressive policy of zero tolerance.

Mr. STUPAK. You would agree with me at a minimum right now we have information that has left its proper secured location, it left the vault, that hard drive, kit No. 2, correct?

Mr. HABIGER. Yes, sir; and what we're trying to find out is how that happened and where those hard drives are today.

Mr. STUPAK. Now in the same area—that is the same place where Wen Ho Lee worked, and he's not been charged with espionage but security breaches involving weapons information, and he's been in solitary confinement in a Federal prison for many months. It appears from the public statements being made by DOE officials that they're already trying to say that this situation is somehow different, someone just lost the information. Is that how a zero tolerance policy is to be enforced?

Mr. HABIGER. Congressman Stupak, we don't know. We've been at this for 7 days. I'd like to think that the aggressive action of both the Federal Bureau of Investigation and Department of Energy will get us some answers soon. Frankly, the polygraphs, being the next step, will allow us to do that.

Mr. STUPAK. Sure, I hope we do get to the bottom of it, but I guess it's a little bit like I've been hammering away for the last couple of years. I've been on this subcommittee now for 6 years. There seems to be this attitude or atmosphere at our labs that things happen, you know. And we try to get some answers, and we'll come back and report to Congress. But we really don't see anything changing. When we say in May 1999 there's zero tolerance and we come back to a situation like this—and I don't know how you can say this is any different than May 1999. It should be zero tolerance. Someone lost the information.

Mr. HABIGER. Sir, and as soon as we find out who lost the information, who misplaced the information, you can—I can guarantee you that very swift, appropriate action will be taken.

Mr. STUPAK. Thank you for the extra time, Mr. Chairman.

Mr. UPTON. You're welcome.

Mr. Bryant.

Mr. BRYANT. Thank you, Mr. Chairman.

I apologize to the panel for being late, but we had, as the Chairman said, other commitments. So I haven't had the benefit of hearing all your statements. I have looked through some of the statements. I do, like my colleague from Michigan, both colleagues from Michigan, the Chairman and Mr. Stupak, have concern here.

It is much like when your house gets broken into, the police officers come out and say, well, you know, we're going to find out what happened here, and we are going to work long and hard hours to get there, and if we catch them we're going to punish them severely. Given the nature of what's been missing here, it's not a burglary of a home; and given the nature of the zero tolerance policy and given the nature of the history of who we're talking about here, it is very disappointing to hear those same things: Well, we're going to find out what happened, and we're working hard to do it right now, 16 hours a day, and when we get them we're really going to punish them.

But I think maybe, General, one of things you said struck me, and it may be an example of this attitude that my friend, Mr. Stupak, refers to. I think you start with the presumption, and that's the key word, the presumption that because we've got good dedicated Americans there, there's an answer. Rather than the presumption that there's been a criminal activity, or something very important is missing, and we better really get going here very quickly. I think that's the example, is the investigation, which anybody that knows, any basic investigatory techniques knows you don't wait 3 weeks to start an investigation after a crime such as this occurs. You get right on it. And I realize there were exigent circumstances involved here, but it just seems to me to have delayed the actual investigation questioning of all those people that had access to this room should not have occurred.

I don't know that it was necessary at your level that this occurred, this decision was made, but at some level of security at Los Alamos, that that decision was made that, it's probably, "somebody's got it home or using it at home or something like that," and that may not have been proper, but the presumption, or the assumption, was there's a good reason out there. Somebody's got it, rather than it could have been taken—it could have been stolen. Somebody could have taken it out, had access.

Again, I think it's the mindset that because these people are good, dedicated Americans who work hard out there, that somebody could not commit a criminal act. Therefore some 2 to 3 weeks we had a delay in the investigation which, if somebody has wrongfully taken it out, it could be no telling where now. We might get that person eventually, and punish them, but this country has lost something very important. Let me go back if I could, Mr. Podonsky, to questions.

In your report, you recommend that the department consider mandating a standdown at all external Web service until significant vulnerabilities are identified or clarified during the inspection that occurred during your inspection and a correction is made to these. Why did you recommend this standdown, and has that been done by the Department of Energy?

Mr. PODONSKY. First of all, we put that recommendation in what we call our opportunities for improvement as the feedback loop to provide the office that we're inspecting, or the Office of Responsibility, to consider that which would be John Gilligan's office. In Mr. Gilligan's corrective actions plan, it does not appear that they are planning to do a standdown. They have other solutions that they have in mind to address the issue that we have identified. We recommended the standdown, getting to the first point of your question, because we felt that until they can do their risk assessment, we would not know what vulnerabilities existed.

Mr. BRYANT. But you have made recommendations in the report, I'm looking here at a question that says—this is kind of skipping on down—six further cyber security enhancements were announced in May 1999 by the Secretary, that they were transferred informally to the management and may have resulted in confusion and lack of implementation. What does that mean to you? What do you know about that?

Mr. PODONSKY. Well, the six further enhancements, there was a nine-point plan, the TriLab nine-point plan from the results of last spring. In addition to the nine-point plan, there were six enhancements that the Secretary put out. Those enhancements were not put out as a policy. They were put out in memorandum form. We took that from an inspection standpoint to mean that they should be followed and should be further memorialized into policy. Mr. Gilligan's office, during last summer, was looking into that and memorializing those things. We felt that the same thing we were doing in looking at it out at the sites and field should be applicable at the headquarters as well.

Mr. BRYANT. There was an issue also about Web pages, some of the Web pages being inside the security wall and some being outside. Are you familiar with that issue?

Mr. PODONSKY. Yes. I am. Let me ask my office director for cyber security to address that.

Mr. PETERSON. That also really relates to your first question on the standdown—that relates to your first question on the standdown. The recommendation was to standdown the headquarter's Web servers located out of what's referred to as the DMZ or the screen subnet. Those we found to have significant vulnerabilities that could either result in a Web defacement or somebody taking over those systems and using them to illicitly attack another Internet entity, and our recommendation was then to do a standdown. We thought it would take a day or two to fix those and then put them back on line securely.

Mr. BRYANT. What is the date of your report that recommends the standdown? When did you recommend that?

Mr. PETERSON. Our initial draft report went out the last week in April.

Mr. BRYANT. Let me go over to Mr. Gilligan. Could you respond to some of these issues, especially some of the recommendations, the implementation of the policy from DOE on those six additional points? Could you just respond in general to those?

Mr. GILLIGAN. Yes, sir, I would be happy to do that. First let me address the Web pages. As the report accurately points out, we have a subset of the Web pages that are supported by headquarters organizations that are in the highly protected enclave we call a screen subnetwork. They've been there for the past year. Those are viewed as being very secure.

There is another set of Web pages that are supported by individual organizations. They are managed by those individual organizations and some of them were found to have significant weaknesses. The recommendation of the independent oversight organization was that a rapid remedy was to standdown, that is, take the Web pages off the Internet and to fix them, that is, fix them individually. The recommendation that I provided to the Deputy Secretary and the Secretary was not to continue to manage these as separate entities, but to move all of the Web pages within the headquarters into this protected area, the screen subnetwork that was found by the independent oversight penetration team to be extremely well protected.

Mr. BRYANT. Has that been done?

Mr. GILLIGAN. That is in the process of being done at present that consists of moving the software, moving, in some cases, the physical computers into the screen subnetwork in order to ensure they are adequately protected. My judgment was that the standdown was not an immediate action. It was warranted because the vulnerability that exists within the headquarters as a result of these Web pages is relatively minor. The threat to the headquarters is that these Web pages could be defaced, which is an embarrassment. There is no loss of operational ability as a result of a Web page not operating.

The other potential vulnerability is that a Web page, or any computer, could be used as a platform for attacking other sites, and in this case, attacking sites outside the Department of Energy, because the Department of Energy's computers are well protected from our Web sites, that is, there is no trust relationship. So we made the decision to rapidly move these Web pages into the screen subnetwork in order to provide the security that I felt was a better solution.

Addressing the second issue which you raised, which was the six further enhancements. The six further enhancements were published by the Secretary with something I contributed to last summer. We have, in fact, embodied those six further enhancements in our policies. The recommendation of the Independent Oversight Group was that perhaps additional policy is needed in order to ensure that all sites clearly understand what is to be implemented in these six further enhancements.

Six further enhancements discuss things like providing configuration control of all computers, providing scanning of the networks, reviewing audit logs and conducting regular audits. All of those requirements are, in fact, codified in our policies. It is the view of my office that rather than change and add to the policies, what we need is guidelines, that is, how to implement the policies on these six further enhancements, again, that are covered in our policies so that there is no ambiguity and we are moving forward to implement that.

Mr. BRYANT. Mr. Chairman, my time is finished. Before I conclude my statement, I would like to ask unanimous consent to add a White House release with regards to the memorandum from the heads of executive departments and agencies and the subject is action by Federal agencies to safeguard against Internet attacks. It's dated March 3, 2000.

Mr. UPTON. Without objection.

[The memo appears on pg. 46.]

Mr. UPTON. The Chair would note that we have two votes on the floor, and I will ask Ms. DeGette whether she would prefer now using 5 minutes or come back after the two votes.

Ms. DEGETTE. Mr. Chairman, I might as well ask my questions now. We still have over 10 minutes. Thank you. Thank you, Mr. Chairman.

General, I would like to follow up on some questions Mr. Stupak was asking you. I guess we're all glad that you're investigating the situation, but given the fact that you discovered the disks missing on May 7, and no one was really told until May 22, and now there's an investigation, I guess I'm wondering what is your timeframe at this point for completing the work you're doing?

Mr. HABIGER. Let me back up, if I may, and tell you—and this relates to Congressman Bryant's question about the timelines between the evening May 7 when the hard drives were discovered missing, and the evening of June 1 when I was notified—or we were notified at DOE headquarters. That is not a good scenario. Someone should have informed us much earlier on in the process.

Ms. DEGETTE. I agree, like maybe May 7 or early on May 8, but that's not my question.

Mr. HABIGER. I want you to know here you had a situation where you had the lab on the verge of burning down.

Ms. DEGETTE. Sir, I understand. I understand what your explanation is for why there was no notification, but my question is, what is your timeframe now for completing the work that you are doing to figure out what happened and how to avoid it in the future?

Mr. HABIGER. At this point, the FBI is now in the lead for the investigation.

Ms. DEGETTE. We're glad about that, too, but what is their timeframe?

Mr. HABIGER. Ma'am, I was called back to take part in this hearing. They begin polygraph examinations beginning tomorrow. They are moving very, very aggressively. I cannot give you an end date.

Ms. DEGETTE. Mr. Chairman, I would just make a request that this committee would consider another oversight hearing in 30 days just to examine the progress. This is such a serious national issue, I think that we should keep monitoring.

Mr. UPTON. You're right.

Ms. DEGETTE. Thank you, Mr. Chairman.

Let me ask you a few more questions. I understand the fire was there when these drives were discovered missing. Where were the kit 2 and the kit 3 hard drives stored during the fire? Where were those stored?

Mr. HABIGER. They were stored in another technical area in a very secure vault.

Ms. DEGETTE. At the Los Alamos site?

Mr. HABIGER. Yes.

Ms. DEGETTE. And out of risk of fire?

Mr. HABIGER. Yes, ma'am.

Ms. DeGETTE. You had said that it was chaotic because of the fire, and that's why your office wasn't informed. Was the lab director informed at that time?

Mr. HABIGER. No, ma'am. I cannot—I've got some information third-hand, but I don't think Dr. Browne was informed until toward the end of the period, the very end of the period.

Ms. DeGETTE. Until close to May 22 or June 1?

Mr. HABIGER. After that just a few days before June 1.

Ms. DeGETTE. Do you have any sense why that happened?

Mr. HABIGER. No, ma'am. I would defer to Dr. Browne.

Ms. DeGETTE. Was Mr. Curran—DOE's counterintelligence specialist informed?

Mr. HABIGER. No, ma'am.

Ms. DeGETTE. Who, if anyone, was informed?

Mr. HABIGER. On the evening of June 1 is when we first discovered that there was a problem.

Ms. DeGETTE. To your knowledge, between May 7 and June 1, no one higher up was informed?

Mr. HABIGER. That's absolutely correct.

Ms. DeGETTE. Is what you were investigating why that happened?

Mr. HABIGER. The primary concern is to get this classified data back.

Ms. DeGETTE. I would agree, but in my experience, when you've got classified data in the form of disks and it's gone from May 7 until June 1, it's going to make the job of getting that data back much more difficult. Would you not agree?

Mr. HABIGER. I couldn't agree more.

Ms. DeGETTE. So therefore, it would seem to me that a second, and almost equally high priority would be trying to determine why the gap, the almost month—the 3-week gap, occurred because in the future, if you have gaps like this, it would make it virtually impossible to get data back, correct?

Mr. HABIGER. I would put the priorities getting the information back, finding out who was responsible for that data, or those hard drives being put in a place where they shouldn't have been. And then the third priority is your area that you're getting into now.

Ms. DeGETTE. General, there is a clear protocol in place that required contractors like the University of California and program offices to inform your office immediately when this type of classified information is missing, correct?

Mr. HABIGER. Within 8 hours.

Ms. DeGETTE. Within 8 hours. And have you ever been informed of these kinds of breaches in the past?

Mr. HABIGER. Yes.

Ms. DeGETTE. Was it done within 8 hours?

Mr. HABIGER. Yes.

Ms. DeGETTE. Do you think this is just a one-shot situation or do you think there is a bigger problem?

Mr. HABIGER. At this point I don't know because the focus, as I said, has been where are the hard drives, who is responsible. The process will take its turn and we'll take the appropriate action. The lab director will take the appropriate action.

Ms. DEGETTE. Mr. Podonsky, do you have any views on that issue?

Mr. PODONSKY. We have not been involved in this investigation, so to answer the question, we have no—we don't have any more information than what you've heard this morning.

Ms. DEGETTE. Now, we've heard that Mr. Curran has told the press that there's no evidence that this is espionage, and someone else said the disks are just lost. Do we have any evidence that this is not espionage or theft for money?

Mr. HABIGER. Ma'am, before you came in, I covered that in a very generic sense, and this is not the forum to get into it, but looking at what we know at this point, it does not appear, as Mr. Curran pointed out, to be espionage.

Ms. DEGETTE. I assume you would want to treat this as a potential case of espionage.

Mr. HABIGER. That's correct. I'm not speaking for the Federal Bureau of Investigation, but that's how the case would be characterized by them.

Ms. DEGETTE. Thank you. Thank you, Mr. Chairman.

Mr. UPTON. The Chair would note there are at least two votes on the House floor. We'll recess until 10:50.

[Brief recess.]

Mr. UPTON. We do not expect votes for an hour or 2, so we'll be done by then, I hope.

Mr. Burr is recognized for questions.

Mr. BURR. Thank you, Mr. Chairman. General, welcome again.

Mr. HABIGER. Good to see you again, sir.

Mr. BURR. Glenn, we always welcome you back. I'm hopeful there's a point where maybe we're not sending you out to do evaluations, that, in fact, we're confident on the process that we've got. Clearly with the news cycle in the last 24 hours, there are some questions that I've got to ask about that probably would be better directed at the General. And I'll try to get refocused back on the DOE headquarters issue.

General, it's been stated that there was a date that they knew that these drives still existed in a secure vault. Was that April 7?

Mr. HABIGER. On April 7, sir, there was an inventory by members of the team, the NEST team, in which the individual who conducted the inventory has indicated that he saw the disk. Another inventory was conducted on April 27, and the individual at that time, a different individual, didn't actually see the disks. His statement was along the lines, if the disks were not there, it would have created a very aggressive reaction. So he remembers doing the inventory, but he doesn't remember actually seeing the disks.

Mr. BURR. Without getting into specifics about what were on these disks, we know they were related to NEST scenarios. Is there any reason to believe that an individual at the facility would have needed access to that particular disk for purposes of something they were working on?

Mr. HABIGER. From the information I've been exposed to in a relatively short period of time, those disks were taken out from time to time to be updated with more current information, and they were taken out by certified people for training purposes.

Mr. BURR. When I was at Los Alamos, we didn't visit that particular vault. We did do several vaults. We also did a reference room or library room and the security was extremely tight, even for us to enter. And we walked through their scenario of if an individual—if a scientist at the facility wanted to take out that information, what's the process they would go through? There was one person in that room whose responsibility it was to account for everything. Things checked out, to make sure they were checked back in. I'm sure there was additional security to make sure it didn't go offsite. My question would be, what was the process in this particular vault when an individual took something out and then replaced it. Is there a record that we can go back to?

Mr. HABIGER. No, sir, there's not.

Mr. BURR. Can you explain to me why for the reference room, the library room that was frequently used, that we would have a process that followed the movement of these papers, but why there wouldn't be a process that followed the movement of hard drives?

Mr. HABIGER. My observation goes along these lines. The vault you're talking about, you're talking about virtually thousands of people who have access, and the vault I'm talking about, the people who had unescorted access to these kits was less than 30.

Mr. BURR. Does it not—in hindsight, I'm not asking you to put yourself before it—in hindsight, does it seem like a reasonable recommendation that we track who removes that type of sensitive information and when, and potentially when they return it?

Mr. HABIGER. Yes, sir. This is one of the many things that we are looking at to change as a result of this particular incident.

Mr. BURR. Is it the responsibility of DOE officials at Los Alamos or the University of California officials?

Mr. HABIGER. University of California.

Mr. BURR. To account for all the items?

Mr. HABIGER. Yes, sir.

Mr. BURR. Let's go back to this period of delay, and we all followed the fire. Should we be worried that there was a security breakdown during this fire episode at Los Alamos?

Mr. HABIGER. I talked on a regular basis to the director of security at Los Alamos during the fire. All security systems were up. Some compensatory measures had to be taken in a couple of areas which I was fully in agreement with.

Mr. BURR. If I understand it, correct me if I'm wrong, this vault facility is in the main building?

Mr. HABIGER. Yes, sir.

Mr. BURR. I guess close to where that library reference room was?

Mr. HABIGER. Yes, sir.

Mr. BURR. Just simply because of the work space, and that was not a building that was left unsecured at any time.

Mr. HABIGER. At any time, no, sir.

Mr. BURR. Was it ever a building that was evacuated of the people? I remember it being so far away from the forest.

Mr. HABIGER. During the fire, there was no one in that building, but the security systems were all up and running. Inside that vault, Congressman Burr, were sensors, motion sensors, infrared sensors that had to be turned off before anyone had access to the vault.

Mr. BURR. Clearly, there was no indication of a security breach that happened?

Mr. HABIGER. No, sir.

Mr. BURR. Let's go to this delay in notification. What is the explanation that the University of California supplied DOE on why they waited so long to tell DOE officials?

Mr. HABIGER. We have not gone down that path. As I indicated, I think, just before you came in, I was not pleased with the length of time that it took before I was notified, before my office was notified, which was on the evening of June 1. During my almost week's stay at Los Alamos, we were focused on three major considerations, the first being where are the disks, and who is accountable for the disks not being where they are supposed to? As we go down the path and we have a very structured inquiry process, part of that process is to come up with explanations for the kinds of things that you are identifying now.

Mr. BURR. I don't want to seem too simplistic, but I put myself in charge of the Los Alamos lab. I envision being in a situation where there's a month's delay before I notify the Department of Energy that high level security hard drives are missing, and I envision the first question that I'm asked, why did it take you so long to inform us? I would take for granted that question was asked. If there wasn't an answer, that's fine, but clearly I think that—we have reason to be concerned because the last time we saw a delay like this was whether we sold a computer to an exporter of Chinese relationship and, you know, when we got through the whole process, we learned that the delay in notification, especially of us, was in hopes that they would retrieve it before anybody found out about it.

Is this one of those situations where there was a hope by officials that the University of California and at Los Alamos that they would find the disk and not have to report it?

Mr. HABIGER. I don't want to put words into Dr. Browne's mouth, but my observation is that scenario that you're just describing.

Mr. BURR. Let me—I thank you for that. I do. I don't think it's any member's intent that we are going to solve this case today, but we appreciate your willingness to let us explore some of the questions.

Mr. Chairman, do I have time to go into some of the headquarters' questions?

Mr. UPTON. Can we go another round and you can do that?

Mr. BURR. I would be happy to do that.

Mr. UPTON. Mrs. Wilson.

Mrs. WILSON. Thank you, Mr. Chairman. Again, I appreciate your willingness to let me ask some questions here today.

As I said in my opening statement, I don't intend to go into some of the details of the most recent incident in Los Alamos, because the questions that I want to ask are very specific, and I don't think that the answers would be appropriate in an open forum. But I think we have summarized pretty clearly what the questions are from this committee's point of view and from my point of view. What happened to those hard drives? Is there a compromise to

America's national security? Who is accountable for it? And how are we going to make the systemic changes needed to make sure it doesn't happen again? And did the notification procedure work?

As I understand it, John Browne, the director of the lab, didn't even know they had a problem until May 31, which is the day before he informed you which means there's a problem lower down within the lab on processes of notification. I understand completely that an investigation could not have been done fully until after the fires were under control, and I think all of us in this room understand that, that you can't do the arson investigation until the fire is out. At the same time that doesn't preclude prompt notification that we may have a problem, and I think those are all legitimate questions we're going to be seeking answers to.

I'd like to focus on a couple of other things from your testimony in the time that I have available. First, this question of funding for cyber security at the Department of Energy. I note from the testimony, particularly General Habiger, yours, concerning the need for supplemental funds. I went back and checked my records, because this was an important issue for me. According to my records for fiscal year 2000, the supplemental requested by the administration—now, you may have asked for more money from the Office of Management and Budget, but it may not have gotten approved—because the administration requested $4 million for cyber security from the Congress. I thought that was way too low, and so several of us from this Congress met quietly with folks who know a little about cyber security and the problems at the nuclear weapons labs, and they confirmed that that was way too low.

I made a request of the Appropriations Committee in the Congress for $90 million in supplemental funds for cyber security for the Department of Energy, and the House approved $45 million for cyber security. That's currently sitting over in the Senate, and pieces of it may be pulled out and added on to one of the bills that we're about to work on in the next couple of weeks here.

I guess what I want to know is, what are you talking about with $35 million? Is that what you asked OMB for and are you now going to continue to support the administration's $4 million request? Are you going to support what the House put into the bill, which is $45 for cyber security immediately?

Mr. HABIGER. We're talking about fiscal year 2000 amendment——

Mrs. WILSON. Current fiscal year, yes.

Mr. HABIGER. We submitted a request for $65 million for security in the Department of Energy in that supplemental, $65 million. We received $10 million of that $65 million. Thirty-five million of that was for cyber security. The $10 million that we got was not directed toward cyber security. I personally directed that $7 million of that $10 million be dedicated to cyber security. That is what, as I understand it, Congresswoman Wilson, came over on July 13 of last year.

Mrs. WILSON. July 13, 1999?

Mr. HABIGER. Yes, ma'am.

Mrs. WILSON. You're talking about 1999 money, not 2000 money?

Mr. HABIGER. Supplemental 19—an amendment for fiscal year 2000 that was submitted on July 13.

Mrs. WILSON. Gentlemen, without meaning any disrespect, I think you may want to go back and talk to your budgeters about which years we are talking about, and which supplementals we are talking about, because there was a supplemental request for cyber security for the current fiscal year, we are in fiscal year 2000, and it was for $4 million from the administration. That was the request. We upped it to 10 times as large.

Mr. HABIGER. It was—the fiscal year 2000 we submitted on the July 13, 1999, an amendment.

Mrs. WILSON. You are talking about when the budget was initially passed for the current year. I am now talking about the supplemental that is pending in this House currently. The administration only asked us—after all of the Cox report, after all of you went out to look at the labs, after we got all of the reports in that said we were way under our estimate of what we're going to need for cyber security—and the administration's request for a supplemental for what we need right now, today, to get moving and get this thing fixed was $4 million. My sense was that was way too low, so we upped it to 10 times that amount, and we're going to vote on it here. What do you want me to vote on? You want me to back off on this and go with the administration at a $4 million supplemental request or do you want me to keep fighting?

Mr. HABIGER. I would like you to keep fighting.

Mrs. WILSON. Thank you, sir.

With respect to this diagram that we see over here, it has a number of firewalls around the top of it and yet it's got a number of connections at the bottom of it which seem to go to other areas within the Department of Energy and contractor facilities and so forth where they don't appear to be firewalls. Could you talk to me about the vulnerability of the DOE unclassified systems through those other areas?

Mr. PETERSON. For the classified systems or for the—I'm sorry, the contractor facilities, what we're specifically talking about there are local contractor support in the Washington, DC area so a program office would establish a connection with a local supporting contractor. That's not to imply that those go out to the national laboratories or other sites.

The other connection that's shown up there for the DOE business net is to 38 different DOE field sites throughout the country. Now, some of those field sites are collocated behind firewalls with other sites. For example, at Oak Ridge, you'd have collocated there Y 12 and Oak Ridge National Lab, but for the Albuquerque field office, there's no connection to Sandia or Los Alamos. So it's going to vary, but specifically, talking about the connections to the DOE Federal facilities. We have a concern because you're exactly right, there's not a firewall at the headquarters junction where you have these connections, and then they become logically part of your headquarters' internal network. There's no firewalls or security features to prevent access from those remote sites. These—each one of these facilities may have their own firewall. They may have modem connections which then provide pathways into the internal headquarters network, and our concern has been that that risk has not been adequately addressed and considered.

Mrs. WILSON. I ask unanimous consent to ask this one final question. Does that mean that someone can get access to the contractor facility, and then from there get into the DOE unclassified system?

Mr. PETERSON. That would be a concern, yes.

Mrs. WILSON. Thank you, Mr. Chairman. I would like to enter into the record the report of dissenting additional views of the Emergency Supplemental Appropriations Act for the year ending September 30, 2000, where it states very clearly that with respect to cyber security, the committee recommendation for cyber security activity is $49 million, an increase of $45 million over the administration's request of $4 million.

Mr. UPTON. Without objection.

Mr. Green?

Mr. GREEN. Thank you, Mr. Chairman. I ask unanimous consent to place my statement into the record.

Mr. UPTON. Without objection.

Mr. GREEN. General, you seem to want to tell us that the problems at the headquarters are not the fault of poor management and lack of attention but of dollars. That's what we're hearing in response to this morning's article where the Secretary said the committee only approved a small amount of funding for last year. But Mr. Podonsky said these are not high ticket items, and now you say we can fix these problems within 60 days. That doesn't sound like a money problem to me. And is it a money problem or are we talking about something different when you say it can be fixed within 60 days?

Mr. HABIGER. We're talking about two different things, Congressman Green. Had we received adequate funding at the beginning of the fiscal year, we'd have been able to move out quickly in terms of training systems administrators, going out and perhaps finding these problems before Podonsky found them, and I would readily admit that the basic problems involve the organizational issues that Mr. Gilligan talked about, but again, it goes back to a money issue. If we had received adequate funding, I don't—in my judgment, our performance would have been better.

Mr. GREEN. Mr. Podonsky, were these problems caused by lack of money or lack of oversight or management skill?

Mr. PODONSKY. First of all, Congressman, I would like to say that in the 16 years I'm reminded I've been in the department, and have lived through six secretaries, nobody other than Secretary Richardson has applied as much attention in management skill to the security issues as the Secretary. However, having said that, I would also say that my staff concluded that a vast majority of the issues at the headquarters unclassified cyber security were management-related, not financially related. There are some financial aspects to it, but clearly, the fragmentation that exists among the various pods in the headquarters need to be fixed and fragmentation doesn't take money.

Mr. GREEN. You don't have to—a lot of us served with Secretary Richardson and consider him a good friend, and he's diligent and I understand that. Sometimes we wonder, even in Congress, if it's a mistake when we do something successfully.

Let me ask everyone on the panel, it's my understanding that DOE is considering opening the bidding for the contract to run Los Alamos National Laboratory, which is currently held by the University of California, in fact, I understand for the last 50 years. Given the problems that this lab has had along with the new revelations that is in today's news media, would you recommend that this contract be open for bidding?

Mr. HABIGER. Congressman Green, let me tell you right up front, I have not been involved in the contract of the laboratory. At this particular point in time, I have no recommendation one way or another.

Mr. GREEN. Anybody else? Since we seem to have problems at Los Alamos and even Livermore, that if someone has had a certain contract for those years, is it something we can look at the contractor? Is it DOE?

Mr. PODONSKY. I think, Congressman, it gets back to the basic accountability in that people, whether they be contractors or Feds, need to be held accountable for their responsibilities that they are assigned.

Mr. HABIGER. The Secretary has made that very clear on a number of occasions.

Mr. GREEN. One last question, again, raised from the article this morning. I was told that the unit that was lost or misplaced, that the unit was not the one involved in the test at Lawrence Livermore in early May. The article said that it was. Can you state for certain, or is it possible that we may be looking in the wrong lab for it? Maybe it's still in California. Again, since it was discovered missing on May 7 and reported on June 1, is that a possibility?

Mr. HABIGER. Sir, we dispatched two Department of Energy investigators who hooked up with two FBI agents at Lawrence Livermore, and every conceivable place was searched and interviews were conducted. This occurred on Tuesday of last week.

Mr. GREEN. Again, Mr. Chairman, whatever time I have left, I share the concern of all the members of the committee, and because of the nature of what would happen, or what could happen with—we're concerned about rogue nations and things like that, that if a terrorist had the ability to utilize this information on how we would respond to a terrorist attack with a nuclear device. So I would just encourage the Department of Energy and our contractor to do everything they can to make sure that they find it, but also that this doesn't happen again. Thank you.

Mr. UPTON. Thank you, Mr. Green.

Mr. Bilbray.

Mr. BILBRAY. Mr. Chairman, I appreciate your having this hearing. General, I'm not going to ask any questions except for the fact that as a father of five, I sure hope my kids aren't watching and reading about this incident. I only say it because I don't know how many times a parent will say where is the last time you saw it, who was responsible for it, you know, the whole concept we have of personal accountability, and this just really makes it tough for those of us who are trying to teach our children to be personally responsible for their little part of the world that they've got control over.

And this situation just really is inexplicable to a young person, let alone a child, about, well, Daddy, what did the Federal Government do with this? Why is this—why don't they know where their important stuff is? Didn't they clean their room and keep it tidy so they know where they hid it? And I'm just here to listen because I'd like to find more answers so that, God forbid, if they ask me when I get home on Friday what happened, where is it, are they going—who is going to be held accountable, I want to at least have some answers for them, because this thing I think is a whole credibility issue that goes farther than just one department in this government. It really, really hurts our credibility as the servants of the American public and as the guardians of world freedom. I yield back, Mr. Chairman.

Mr. UPTON. Thank you, Mr. Bilbray.

I have a couple more questions. We'll start a second round.

General Habiger, it's my understanding that they knew the disks were there in April. When was the last time that all the disks were known to be accounted for?

Mr. HABIGER. In kit number 2, the last fully confirmed audit was on April 7. We have an unconfirmed audit or inventory by an individual, as I indicated before, said that if they weren't there, he doesn't remember seeing them, but he said if they weren't there, it would have rang alarm bells.

Mr. UPTON. So really not until May 8 did you realize——

Mr. HABIGER. May 7, sir.

Mr. UPTON. May 7 that they were there.

Mr. BURR. Would the chairman yield for one clarification.

Mr. UPTON. Yes.

Mr. BURR. General, was that the only thing in that vault or are there other sensitive documents or disks or hard drives?

Mr. HABIGER. There were three kits in that room, sir.

Mr. BURR. When you say they were a kit, kit No. 1 was accounted for on April 7.

Mr. HABIGER. Kit number 2.

Mr. BURR. Does that tell us that kit number 1 and kit number 3 were not accounted for on April 7?

Mr. HABIGER. That is true.

Mr. BURR. I thank the chairman.

Mr. UPTON. And there was more than just the kits. Could you describe this vault again. Those of us that went out, we were in the library there. The library is sort of the secure room that was there. We did not—I don't believe we saw where this vault was in the building, but is it similar to the other vaults that we saw?

Mr. HABIGER. Sir, it's much smaller. It's about ten foot wide, about 20 feet long there. There were two long tables, a number of shelves, a small two-drawer safe. There were some documents. There were other hard drives.

Mr. UPTON. Is there security outside of the room then as well?

Mr. HABIGER. Yes, sir. Sir, this is a vault. I mean, this is something that, again, in open session without—I'd rather not go into the details, but this is something you and I would take several weeks trying to break into. I'm talking about dynamite and explosives and that sort of thing.

Mr. UPTON. Of the—is it 28 or 26 individuals that have access to it without being escorted?

Mr. HABIGER. I believe the number is 26, sir.

Mr. UPTON. Of those 26, are all of them U.S. citizens?

Mr. HABIGER. Oh, yes, sir.

Mr. UPTON. No foreign nationals?

Mr. HABIGER. Oh, no, sir, no, sir.

Mr. UPTON. I just want to make sure.

Mr. BURR. Mr. Chairman, would you yield? Twenty-six individuals have access to the kits?

Mr. HABIGER. Unescorted access.

Mr. BURR. Are there any other individuals who have unescorted access to the vault?

Mr. HABIGER. 57.

Mr. BURR. 57 to the vault?

Mr. HABIGER. Yes, sir.

Mr. UPTON. They have to be escorted, though.

Mr. HABIGER. Escorted. 57 escorted.

Mr. BURR. My question is, is there a difference in those that have access to the kits and access to the vault? Is it the same list or is it one and the same?

Mr. HABIGER. The people who have unescorted access can open up the vault. The 57 who have escorted access have to have someone who has unescorted access, open the vault and let them in to do what they have to do. This is a good point and I should have clarified it earlier. The vault was a dual-purpose vault. On one side of the vault you had the NEST activities, and on the other side of the vault you had the ASCI, the Advanced Strategic Computer Initiative activities on the other side of the vault.

There is an individual who is accountable for that vault. It's an individual who has unescorted access to the vault, and she is responsible for who gets in there and makes sure that only people—the people that have unescorted access are watched by her if she's in there. If she's not in there, the door should be locked.

Mr. BURR. Unescorted access means they have total access to everything in that vault?

Mr. HABIGER. Yes, sir.

Mr. BURR. The right side and the left side you're describing?

Mr. HABIGER. Yes, sir.

Mr. BURR. I thank you.

Mr. UPTON. Have all the folks with access to the vault been quizzed already?

Mr. HABIGER. Sir, all of the people who have unescorted access have been interviewed. Most of the people, primarily based upon availability who had unescorted access, have been interviewed.

Mr. UPTON. Now they are going back to reinterview all the individuals with a polygraph; that begins tomorrow?

Mr. HABIGER. The FBI is working up a list of people that they will polygraph. The FBI is in charge of the polygraphing process.

Mr. UPTON. I want to go back to the dollar amount that Mrs. Wilson raised with regard to the supplemental. Before I was in the Congress, I served at the Office of Management and Budget. I was very aware of different agency requests that came in, and ultimately what happened to them up on the Hill, and it was one of the reasons that a number of us wanted to go out and visit the labs. Actually, I think it was the hearing that you might have been at last summer, where a number of us indicated we had never been there and we wanted to get a better understanding of just exactly what was there, so we could have a helpful hand in making sure that security was appropriate.

Mr. Podonsky and others provided many details to us. As we undertook the Department of Energy's budget last year, I do remember there were additional requests that came in, but it was included as part of the overall spending bill that was adopted in, I believe it was October, and everything was on the table, and if the administration, I think, had pushed a little bit harder, or even some would suggest pushed, in fact, the full funding amount would have been included as part of the overall bill. But it is sort of surprising that as it wasn't all funded, that the Department of Energy would only—I should say the administration would seek only $4 million, which we have now requested more than 10 times such, but based on the testimony by Mr. Gilligan this morning where, in essence, he indicated that problems were identified a year ago and, in fact, within 60 days, a system would be set up to make sure there wouldn't be any problems and that's without any funding at all.

As we look at the level of funding that we've done with the labs, the labs were very careful to tell us that security was No. 1 and that they would find—they identified a number of weaknesses that were out there and that they would find the resources to fix the problem, no matter what the cost, and, in fact, I think they've done that, would be my sense, as they've testified to us earlier.

I just wondered why isn't A, the same standard there at the headquarters and B, how are you able to do it now? It sounds like you're able to do exactly what you wanted to do without an extra dime coming your way.

Mr. GILLIGAN. Sir, I appreciate the question, and let me if I could, go back and make clear, the request that we made last summer for $35 million as a budget amendment for the fiscal 2000 was something that I personally worked. In fact, my initial recommendation was for $50 million. Working with the Department, we were only able to identify offsets, that is, other budget reductions within the Department to support $35 million. That came through the administration over to Congress. We got 7 million. Of that, $1 million was earmarked for a specific project; so $6 million to be able to dedicate against the priorities that we identified.

Frankly, I was surprised that we didn't get support after we had had the hearings and the discussion, especially in view of the fact that the Department provided offsets, other budget reductions. Those offsets were taken to fund other priorities.

Subsequently I was given an opportunity—I was given a cap of $4 million to identify additional cybersecurity initiatives that we could request in a budget supplemental, and we did.

Now, to address your specific question on the current headquarters review, the significant problems that we've identified, many of them can be fixed with limited dollars, I will readily admit that. There are some significant management issues that we can address in the Deputy Secretary's memo, which, in addition to the policy authority that I have for the Department, now gives me line operational authority for the headquarters computer security. I can now work to put the management changes that need to be in effect to be able to fix most of the problems.

However, I still need additional funding to fully implement protections to solve some additional weaknesses that I am aware of on that picture. For example, at the lower left of that picture, you see a cloud network. That is the DOE network. That network connects our headquarters with all of our Federal operations. That is something I am responsible for. We, in fact, do have a policy, and we have enforced the policy that each of the sites must have a firewall before they can connect to DOE Net. Mr. Podonsky's review identifies that additional security measures would be warranted, and I agree, and that would be to create an additional protection so that one site that potentially is compromised could not affect another site.

That will take funding. That funding is something I have requested now in the 2001 budget, and I would appreciate support for that. So we will be able to implement some of the fixes, some of the configuration management enforcement. Some of the connection policies we will be able to implement. We will not be able to implement some of the full enhancements that I would like to do to get the headquarters up to the level of my comfort without additional funding in fiscal year 2001.

Mr. UPTON. Thank you. I know my time has expired. I'd just like to tell all members that we're looking at having a classified closed briefing with General Habiger on the issue of the missing hard drives, not only with this subcommittee, but also with other members on Intelligence as well as Armed Services, and it could be later today.

Mr. Stupak.

Mr. STUPAK. Thank you, Mr. Chairman.

General, the way I understand it here, there are three kits, two hard drives each. So there's a total of six hard drives.

Mr. HABIGER. Yes, sir.

Mr. STUPAK. Can you tell us when the last time all six were present and accounted for?

Mr. HABIGER. I can tell you that—not all six. I can tell you that 4 of the 6 were accounted for when the lab began their aggressive inventory on the—beginning May 22.

Mr. STUPAK. May 22?

Mr. HABIGER. Yes, sir.

Mr. STUPAK. All right. Why would you take the hard drives out of kit three and put it in kit two?

Mr. HABIGER. So you'd have an operational capability. Remember——

Mr. STUPAK. But then that renders kit three incapable, right?

Mr. HABIGER. The hard drives are all the same. One's primary, one's backup. The concern was to get an operational kit out of harm's way, and so the individuals who went into the vault at 2300 on May 7 made a decision to move the two hard drives.

Mr. STUPAK. All right. Well, move them out of harm's way, we're talking here about a wildfire. From my watching of the news and everything else, it seems like a wildfire is threatening to an area or a place for a day or two because it's a wildfire, and then it moves on. Your testimony is that from May 8 to May 22——

Mr. HABIGER. Sir, the winds were constantly changing, and the winds were up to 60, 70 knots during this period, and initially—and you had massive changes, 180-degree wind changes of these very high winds, and the exposure or the risk to the lab would go up 1 day and down the next, just depending on which way the wind was blowing.

Mr. STUPAK. Well, if it would go up 1 day and come down the next, during that time did anyone make any efforts then to try to locate these disks?

Mr. HABIGER. As far as I know, no, sir, and let me point out that the Los Alamos—the city of Los Alamos and the laboratory were shut down, were evacuated. National Guard troops were in place, State police, to ensure that.

Mr. STUPAK. Okay. Let me just—and I know a statement was made earlier that you can't do an arson investigation while a fire is ongoing. Having been in police work for 12, 13 years, I totally disagree, because during an arson investigation there are things you look for, people around there, the evidence, containers, fire trails, the burn patterns. Those are all key parts of any arson investigation, and I'm sure they are in any investigation. I'm still befuddled why we waited until after May 22 and you not being notified until June 1. I just find that unacceptable and—but I'm sure we can get into that some other time.

Mr. Podonsky, you're in charge of the Independent Oversight for security at DOE, correct?

Mr. PODONSKY. Yes, sir.

Mr. STUPAK. And you spent a lot of time out there last year and after it was determined that classified information was being downloaded into unclassified systems; did you not?

Mr. PODONSKY. Yes, we did.

Mr. STUPAK. One of the things you told the subcommittee in October when we held a hearing on the security situation at the weapons lab was that there—and I am going to quote now—there were weaknesses in access controls at areas where classified weapons information was used and stored. Is that correct?

Mr. PODONSKY. That is correct.

Mr. STUPAK. And that's not a cybersecurity issue, it's a plain old physical security problem. In fact, you were talking about areas exactly like the vault in which the lost hard drives were stored, correct?

Mr. PODONSKY. That is correct, but we were not at the TA three area.

Mr. STUPAK. I know you weren't talking specifically about that vault at that time. It's the idea of the same old physical security problem. Now that we've established that the disks were in the emergency response kit for the NEST team, and the kit was in a locked suitcase-like container with other locked containers inside, these hard drives were in one of those containers. The suitcase, however, was accessible to anyone in the room. We've already established there were keys there, you could get at them. Can you explain to me then how a situation could have been allowed for this type of security breach? I mean, if it's plain old physical security, and that was a concern a year ago, why would we have the keys right there, accessible, attached to the kits or hanging on the wall? It just seems like a great opportunity to access it by somebody who should not access it.

Mr. PODONSKY. I can answer generically since we are not directly involved in what's currently under investigation. However, I will tell you in August when we were there, they were rated satisfactory, the overall site security, and then again in December, and that was based on the performance that we saw at the sites within the laboratory that we inspected. We maintain and believe that that was a satisfactory performance.

There is a human element in security, and that's something that is always unpredictable. Obviously, as I said, we don't have the details of what's going on in the investigation, but we had seen, just like in the downloading of classified to an unclassified Net, there is always that human element, regardless of all the administrative controls that you put in.

Mr. STUPAK. Exactly. There's a human element. I think when we raised it earlier, I was reminded that these are good, hard-working, honest people. No one up here is saying they're not, but the fact remains we still have two hard drives missing that can't be accounted for, that can't be remembered where they are.

And explain something else for me if you can, and maybe I'm—explain how a nuclear weapons laboratory can have a satisfactory security program, but can lose or have removed weapons, design and intelligence information such as on these hard drives? How can they get a satisfactory?

Mr. PODONSKY. At the time that we inspected them, they were performing at a satisfactory level, and all the things that we tested, the guards, the cybersecurity, the material control accountability, they were not only in compliance with the DOE requirements, but they were performing well, albeit this latest news event that just occurred is not a satisfactory situation, but that does not, in our view, taint the entire laboratory's performance. It does call into question a lot of other issues that I'm sure General Habiger will talk in a closed session.

Mr. STUPAK. In the previous hearings we've always brought up this atmosphere that exists at the lab, rather relaxed atmosphere, and I've been one who always talked about accountability and responsibility, and then we continue to see these satisfactory, satisfactory, and then we hit another embarrassing-type situation. So I guess that goes back to that human element. No matter how honest or how well we think employees are, there's still going to be a degree of human element that you can't put satisfactory on. Is that a fair statement?

Mr. PODONSKY. I would say there's a—with any corporation, in DOE in particular, as we've seen, there's some very dedicated people there that are doing the job for very noble reasons, and there's always going to be the human element that you cannot put a satisfactory on.

I am reminded when we used to do safety oversight, we had a number of very serious and near fatal accidents at the laboratory. Not everybody took safety seriously until it happened to some of their own researchers. So that human element is something that it is very difficult to quantify. So what we do is we don't just look at technical systems, we look at management systems. We try to get to the root cause. We're not at all trying to indicate that we hide behind the curtain of the human frailties, but that's something that has to be considered.

Mr. STUPAK. Thank you, Mr. Chairman.

Mr. UPTON. Mr. Burr.

Mr. BURR. Mr. Gilligan, let me attempt to answer a question you raised or a statement that you made, and this is a response from me personally. You said that you were surprised that the budget request was not fulfilled, and I would only share from a standpoint of somebody that I think has been in every security briefing that we've had, open or closed, has followed the process to the extent that over the break I traveled to California for a three-stop tour in 2½ days, and has followed not only the General's suggestions, but the Secretary's statements, that many of the things that were stated up front have not been fulfilled.

I am not here to judge whether they should have been made or should have been carried out, but we made some changes along the way, and that's understandable as we're addressing a crisis of the moment. I think the lack of any specific funding that might not have made it is a lack of confidence that we have the right plan in effect, or that we're concerned on whether we will implement what it is that we have endorsed, or there's not that degree of need to accomplish what has been explained to Congress.

So the challenge is indeed on your part and on the part of General Habiger and of the Department of Energy to make sure that every Member of Congress understands what the cost of the process is, and that may be a more elementary challenge on your part than we have had in the past, but we are not going to knee-jerk to a crisis that exists. We're going to ask for the documentation, and we're going to ask for the accountability that what you tell us is accomplished.

Let me move back to the current situation for just a few more questions, General. What do you mean by escorted? When a person is escorted, what does that mean, into that vault?

Mr. HABIGER. They have to be accompanied by someone who understands the security requirements.

Mr. BURR. Would that individual have to be on that list of 26 individuals?

Mr. HABIGER. Yes, sir.

Mr. BURR. For secure access by themselves?

Mr. HABIGER. Yes, sir.

Mr. BURR. You mentioned, I think, ASCI information additionally was stored in that vault?

Mr. HABIGER. Yes, sir.

Mr. BURR. Is that accounted for and secure today?

Mr. HABIGER. Yes, sir.

Mr. BURR. All of it?

Mr. HABIGER. Yes, sir. As a matter of fact, the laboratory in the nuclear weapons arena, Dr. Browne directed as of 1700 hours yesterday that a 72-hour lock-down of the nuclear weapons area be accomplished, and that all plans, security plans, be reviewed, and that all classified media, documents be accounted for. That's to be accomplished over a 72-hour period.

Mr. UPTON. Would the gentleman yield?

Mr. BURR. Yes.

Mr. UPTON. When somebody is in the vault, and they are to be escorted, does the escort then have to stay with that individual the entire time they are within the vault?

Mr. HABIGER. Yes, sir; again, 10 feet wide, 20 feet long.

Mr. UPTON. So if you need the escort, there's always at least two people in that room?

Mr. HABIGER. Absolutely, sir.

Mr. BURR. General, if you can't answer this, I understand it, we'll address it later, but after an individual has possession of this hard drive, how easily is it usable? Is it a plug and play?

Mr. HABIGER. Yes, sir.

Mr. BURR. Okay. Was this the most sensitive information in the vault?

Mr. HABIGER. Yes, sir.

Mr. BURR. Let me ask you, you referred to the fact that the FBI has taken the lead in the investigation, and you expect next week for the FBI to begin a polygraph process.

Mr. HABIGER. Tomorrow.

Mr. BURR. Tomorrow, once they have identified individuals. We know the record with polygraph as it relates to our scientists. This is not something that they do enthusiastically. Do you have any reason to believe that any of the individuals that will be targeted would object to this initiative?

Mr. HABIGER. I will give you a very definitive answer in closed session, sir.

Mr. BURR. I thank you for that.

Let me move, if I could, to why we're here today. Glenn, last time you testified here, I believe you very emphatically told us that the message was getting out on security, that that had been heard, and today you're telling us that DOE headquarters heard the wake-up call. Is that right?

Mr. PODONSKY. Yes, sir.

Mr. BURR. If DOE headquarters really heard that call, then why do you find such a bad situation involving very basic principles of computer security?

Mr. PODONSKY. Well, sir, as I started to mention in my response to Congressman Green, I'd like to iterate, in all the time that we've been in the Department, we've seen some very egregious management systems in place, a lot of repeat issues that should have been dealt with over the last 16 years. Many issues have been written about in our oversight reports. Various administrations did not have it high on the priority.

For obvious reasons, this administration, together with this Congress, has focused a great deal on security in Department of Energy, and to you all's credit as well as this Secretary, we have seen a quantum change. It doesn't mean they are there where they need to be, but clearly the headquarters, the responsibility that John Gilligan has being further clarified by his Deputy Secretary Glauthier's memo will further help him do the job that he was hired to do, but in addition, he and his staff have been focusing on the field extensively. So quite candidly, until the management processes were in place, we did not see that they were going to be very successful at bringing the headquarters into the same level that the field is now getting into.

We believe with the corrective action plan that Mr. Gilligan's office has prepared, if all the items in there get carried out, we do believe it's going to be going in the right direction. That's why we say that we've seen a difference. It is taken in respect to what we've seen over the last 16 years.

Mr. BURR. Most of us who have served for several years consider Bill Richardson to be a friend, and we know that every effort he goes out on is genuine and passionate. So I think we would hold in the same regard the Secretary's willingness to address this problem. The follow-through is something that this committee continues to be baffled at, and I would only point to the March 3, 2000, memorandum from the White House, and that memorandum, in the last paragraph it said, accordingly, I've asked each Cabinet Secretary and agency head renew their efforts to safeguard their department's or agency's computer systems against denial-of-service attacks on the Internet, stepping up the awareness of a security breach.

That was March 3, 2000.

It also said, I have asked my Chief of Staff John Podesta to coordinate a review of the Federal Government vulnerabilities in this regard and report back to me by April 1.

[The information referred to follows:]

THE WHITE HOUSE
OFFICE OF THE PRESS SECRETARY
March 3, 2000

For Immediate Release March 3, 2000

MEMORANDUM FOR THE HEADS OF EXECUTIVE DEPARTMENTS AND AGENCIES

SUBJECT: Action by Federal Agencies to Safeguard Against Internet Attacks

America and the world have benefited tremendously from the amazing advances we have seen with the Internet and computer technology. But with every new technological advance there are new challenges, and we must meet them—both Government and the private sector—in partnership.

Following recent Internet disruptions, I met with experts and leaders of the information technology industry so we could work together to maximize the promise of the Internet, while minimizing the risks. These Internet disruptions high-light how important computer networks have become to our daily lives; and how vulnerabilities can create risks for all—including the Federal Government.

Accordingly, I ask each Cabinet Secretary and agency head to renew their efforts to safeguard their department or agency's computer systems against denial-of-service attacks on the Internet. Within legal and administrative limits, attention should also be paid to contractors providing services. The Federal Computer Incidence Response Center (FEDCirc) and the National Infrastructure Protection Center (NIPC) have available software tools to assist you in these efforts.

I have asked my Chief of staff, John Podesta, to coordinate a review of Federal Government vulnerabilities in this regard and to report back to me by April 1.

WILLIAM J. CLINTON

Mr. BURR. Mr. Podonsky or General Habiger, can you share with us what Mr. Podesta reported to the President relative to the state of security at the Department of Energy?

Mr. GILLIGAN. Sir, I'd be happy to tell you. In fact, I was one of the authors of that memo that the President signed. Under my role as cochair of the Federal CIO Council, Security, Privacy and Security Infrastructure Committee, I have a responsibility to help advise the administration across the Federal Government. We prepared that memo for the President. We prepared a process working with Office of Management and Budget, Mr. Podesta's staff, to get reports from each Federal agency. Within the Department of Energy, I coordinated the response. We sent out guidance to each of our field organizations, specific technical guidance on how to prevent denial-of-service attacks. It is a particularly difficult, technically challenging——

Mr. BURR. I take for granted that the April 1 deadline for Mr. Podesta to get back to the President was a status report, are we secure.

Mr. GILLIGAN. No. The status report was on those actions that have been taken. Security is not a binary function. It is not we are 100 percent secure or we are 100 percent insecure. It's a relative activity. It's a very complex set of technical issues that are involved.

The status report that was asked for was what was the response within each agency to address denial-of-service attacks, and within the Department of Energy we reported that each of our organizations had taken the guidance that we had issued, they had responded to the guidance in a variety of ways, many running specific software checks against all of their systems to look for potential vulnerabilities that could be exploited, to look for configuration controls that would, in fact, allow us to prevent denial-of-service attacks.

Mr. BURR. Did the Department of Energy make the April 1 deadline?

Mr. GILLIGAN. Yes, we did.

Mr. BURR. Glenn, your review of security was at the end of April?

Mr. PODONSKY. Yes, sir.

Mr. BURR. At that time did you find Web servers at the Department of Energy that could access other agencies?

Mr. PETERSON. We found Web servers, again referring to our diagram, out in the public area outside of the screen sub-Net, that were vulnerable to attack. We proved that by taking over one of those machines, and we could have used it to attack a different agency.

Mr. BURR. You could use them to launch a denial-of-service attack on other government agencies?

Mr. PETERSON. That is correct.

Mr. BURR. Now, is that what you reported to Mr. Podesta?

Mr. GILLIGAN. The report back to Mr. Podesta did not address every individual computer within the agency.

Mr. BURR. So what was the President asking for in this memorandum? I mean, I take for granted he was probably asking about some of the most sensitive secure areas. We're doing an assessment of unclassified areas and just our Web servers. We were vulnerable to exactly the thing the President said in his memorandum, which was denial of service existed.

Mr. GILLIGAN. Each of the sites reported the steps that they had taken. The headquarters organizations, plural, reported those steps they had taken to respond to the denial-of-service attacks. We did not at this juncture verify each and every computer the fact that something——

Mr. BURR. If you knew that those existed when you put this report in, why was Mr. Podonsky's review of the system needed if you knew where we were vulnerable?

Mr. GILLIGAN. I am not sure, sir, I understand your question.

Mr. BURR. You responded to Mr. Podesta for the purpose of his reporting to the President the status at DOE by April 1.

Mr. GILLIGAN. That's correct.

Mr. BURR. At some point thereafter Mr. Podonsky's still doing a review of unclassified systems at the Department of Energy, and he finds vulnerable areas. I guess the question is, did you know about those vulnerable areas when you reported to Mr. Podesta?

Mr. GILLIGAN. Sir, today and in the future there will continue to be vulnerabilities in our computer systems. That's the state-of-the-art. There are vulnerabilities in the computer systems that are run by this Congress, but that's the state-of-the-art. The securing of these systems is a continuing process. The report back to Mr. Podesta identified those processes and the verification that each of our sites had done. It did not say that there were no vulnerabilities. In fact, there are vulnerabilities that continue to be discovered and exploited.

Mr. BURR. Is the vulnerability—and I am not a techie, clearly you are—is the vulnerability of a Web server and its potential use to launch attacks a new phenomena, or is that something that has existed since Web servers have been out there?

Mr. GILLIGAN. The potential to use——

Mr. BURR. Is that the last place we look for a vulnerability, or is it one of the first places?

Mr. GILLIGAN. The Web server is generally not a high risk, a highly vulnerable computer, because of the limited functions it performs, and in general, Web servers are intended for public access, and the protection on those is primarily to ensure that the information content that is primarily read only is, in fact, preserved.

Mr. BURR. Let me turn to Mr. Podonsky, who did the investigation. Is a Web server a tool that one should be concerned with if that Web server is unsecured and can be used to launch attacks on?

Mr. PETERSON. Absolutely. For one, it could be an embarrassment to the Department having it defaced, and then the second one is to have our resources from the DOE to be used in an illicit manner.

Mr. BURR. Let me just read from your report if I can. I quote: Most of these Web servers were found to be vulnerable to common hacking exploits, and some contained vulnerabilities that could allow any Internet user to gain system administrator-level privileges. With this level of privilege an attacker could deface or shut down the Web site or configure the server to launch attacks against other Internet entities causing public embarrassment to DOE.

So, in fact, you did put it in your report—in the way that you've stated it, it sounds fairly serious.

Let me just ask one last question, Mr. Chairman.

Glenn, your report also concluded by stating this, and this is alarming to me, it really is: Senior management attention is needed to establish a management structure conducive to effective unclassified cybersecurity at headquarters. Now, we have all praised Bill Richardson quite a bit. We have a lot of confidence in you, General. We have tremendous confidence in a lot of folks at the Department of Energy. But, Glenn, I have got to ask you, what led you to put that in your report, that senior management's attention is needed? We've had a series of security breaches, of management blunders, I think. Nobody has ever questioned the commitment of the Secretary, but something led you to say senior management doesn't get it yet. Who were you describing when you used the term "senior management"?

Mr. PODONSKY. Let me answer your question in the following way. Last week I met with General Gordon, and one of the things he asked me about the new NNSA, what are some of the first things he ought to do. He was planning to go and do some tours of the sites around the complex, and I suggested that he first needs to take a look at headquarters, and he needs to take a good hard look at how headquarters operates. And I would say that what we were aiming at is when we looked at what is the root cause, General Habiger and John Gilligan and all the folks that are dedicated to doing the right thing in the Department have mostly been focusing outside the headquarters is what our assessment was, and there's an awful lot of organizations within that Department across the way there that may need to be working all in unison.

So our focus was that senior management at headquarters needs to also take a look at the operation of the Forrestal as well the Germantown building, not just the field offices.

Mr. BURR. Technical question. My understanding is that DOE contractors in some way, shape or form are linked to regional offices and/or headquarters of the Department of Energy. Could those links also be used to launch attacks from, or could those links be used to exploit any security measures that we have in place?

Mr. PETERSON. We are concerned with the links from the exploitation aspect. Obviously it broadens your network perimeter, and then it will allow you—if you find the weakest point, then it allows you into that broad perimeter of that network, and then if you have enough time and skill, then you can take over a machine, a computer, and then use that to launch an attack against the Internet site. So that's definitely a concern.

Mr. BURR. General, let me just make one last statement, if I could. I do hope we go to a closed session, if not today, very quickly.

I would only say this, that for a vault containing high-security information, one that we were concerned enough with to go through a process of individuals who could visit it, No. 1, and from that list who needed escorting, that apparently we have a full-time person who oversees the entry to that vault and the exit to that vault, it is amazing to me that there's not some record of who accessed it when and if anyone removed something from that vault, and if so, when it was returned. If this were some type of nuclear material of which we have identified a similar set of scenarios that we have addressed, one of the remedies was that it no longer goes without some type of cataloging of who went, when they went, what they did, when it was returned, if it was taken off premises. I do hope that that's a procedure that will change, and if it can't be accomplished through our current contractor, I hope the Department of Energy will be brave enough to review this contract and to look at somebody that can run a facility with the type of procedures that we need, as Mr. Gilligan said, in an ever-changing technological world that every day we're faced with a new risk and a new challenge.

And with that, I thank all four of you, and I yield back.

Mr. UPTON. Thank you.

I just want to note, thanks to the membership of Mrs. Wilson on the Intelligence Committee, we've been able to secure the intelligence room in the Capitol until 2 o'clock. General Habiger, would you be able to come maybe at like 1 until 2:00?

Mr. HABIGER. Sir, at your convenience.

Mr. UPTON. Okay. Well, we'll put a notice to all members of the full committee that that is available, and you know where it is in the Capitol; do you not?

Mr. HABIGER. I'll find it.

Mr. UPTON. It's hard to find. I'm sure David can help you.

We'll yield at this point. I am going to leave here shortly. Mr. Burr is going to take over the chairmanship, and I will see you at 1 o'clock, and at this point we'll yield to Mrs. Wilson, who has got a couple more questions.

Mrs. WILSON. Thank you, Mr. Chairman. I do have a couple of more questions, particularly about cybersecurity at the headquarters. And, General, I have a lot of sympathy for your situation, trying to get a job done and convince—I have been in that situation myself—trying to convince the budget guys that you have got a job to do and you need the resources to do that job and so forth. But I do think it's important to make sure this chronology is in the record with respect to cybersecurity, and I think I have kind of compiled my own summary of it at this point. And I think it's important for everybody to understand what happened in 1999 and where we are now.

In January 1999, the Cox report was finished in its classified form, briefed to the administration and key Members of Congress.

Of course, by that time, the administration's budget request was already in and up here, and there are a number of requests that come in to amend that throughout the year as we are beginning work on it.

On May 14, 1999, the Department of Energy requested an amendment to the President's budget request for cybersecurity. That went to the energy and water committee, and that request was for $8.5 million, and it was fully funded.

May 25, the Cox report is publicly released in its unclassified form, and there is a firestorm of hearings and investigations and responses in both the Defense Committee, the Intelligence Committee and this committee all the way through June. It affected the defense authorization, intelligence authorization and the appropriations bill.

On about July 13, as I understand it, there was a request in the energy and water committee for $35 million, General, for your office. It was listed as security. The committee asked for further justification and breakdown and were not able to get it. This is 24 hours before the markup in subcommittee. It was not listed as for cybersecurity. It was for the funding of your office, and I have no doubt at all that your office needs that funding to do your job. Without that supported breakdown, you were given $7 million initially from that subcommittee mark, but it wasn't cybersecurity, it was for your operations in your office, and I understand that's entirely legitimate.

It then goes through the House and over to conference. I would note that there's a man named Senator Pete Domenici, who I know pretty well, who is on that conference committee, and if there was a shortage for cybersecurity, particularly for the nuclear weapons complex, it would not have been particularly difficult to get that put into the bill.

In the fall, the labs continue on looking at cybersecurity and their needs and making plans and assessments of the costs of this whole thing, and when we come back in January, me and a whole bunch of other folks were expecting a major request for a supplemental, particularly related to the cybersecurity, but in February we get the White House's supplemental request, and they only asked for $4 million for cybersecurity.

We then get a group together here of experts and others and ask in early March, is that adequate? Is this real? And the answer is quietly, no, it's not. It's not the real number, it's not the real need. So we make the request of Energy and Water in a separate supplemental to bump that up significantly. I ask for $90 million; $45 million is added specifically for cybersecurity.

I think that is important as a chronology because, now, I think there's sometimes an attempt to shift blame around. And I understand that you're in a difficult situation. You have to get up and operating as a security office, but with respect to cybersecurity and the requests that come in for cybersecurity, I think the appropriators have been pretty good at working with those members like myself who are concerned about this issue and fully funding the requests that are identified as protecting our security programs, our computer security, and we'll continue to fight those battles up here and get the money that's needed. I frankly wish that I had more support from the administration when it comes to really identifying the actual costs that are going to be needed, and I'd appreciate it if you'd take that one back.

I do have some questions concerning this chart, some more things. First from Mr. Gilligan, is there a single unified risk assessment and a security plan for the headquarters network as a whole?

Mr. GILLIGAN. Congresswoman Wilson, there is not, and, in fact, I think that's one of the observations that the independent oversight review points out that I agree is a weakness in our implementation. If I look at how we implemented cybersecurity policies within the headquarters, each individual subordinate organization in the headquarters implemented the policies individually. So there are multiple risk assessments. There are multiple cybersecurity plans, there are multiple cybersecurity implementations, and I think Mr. Podonsky's team correctly identifies this as an overall weakness because we have some offices who do a very good job of implementing those plans, correcting the vulnerabilities, and other offices who have not done a good job, but it becomes a shared risk.

So the action that was taken by the Deputy Secretary in essence expands my job, so not only am I to have policy responsibility for the entire Department, but I now have operational responsibility which I did not have previously for the entire headquarters. In the past I had operational responsibility through an operations organization that happens to be attached to me for small subsets of the headquarters, and, in fact, those portions of the headquarters were viewed as very strong in the independent oversight review, yet they were vulnerable to other offices who had weaker security. So now that I have responsibility for the operational security of the entire headquarters, we can do one plan, one risk assessment, one set of policies and procedures, and I can enforce those policies and procedures across the headquarters.

Mrs. WILSON. When were you given that additional authority?

Mr. GILLIGAN. On June 8.

Mrs. WILSON. Okay. Does DOE have a comprehensive list of the external connections so that anything that enters those circles or those subcircles here—do you have a comprehensive list of external connections?

Mr. GILLIGAN. Ma'am, we have a list. I would not say that it is a comprehensive list. I think that is a continued vulnerability. The Internet networking technology that we have today lets connections be made quite rapidly, and that would be part of the objective of establishing a very rigorous perimeter across all of the headquarters systems and a what is called connection policy which we can enforce, which would, in fact, then allow us to map what are all the external connections, do they, in fact, conform to the security provisions that must be in place before an external connection is permitted, and that's more part of the activity that's under way now.

Mrs. WILSON. With respect to the additional authority that you have been given on June 8, and I also have some sympathy for your situation being responsible for something, but I would guess a lot of the guys who have to implement this don't really work for you, they still work down in DP and IA and NN and those kinds of things. Is that right?

Mr. GILLIGAN. That's correct. My office now has overall responsibility. We will still work with the individual offices, but now I have the accountability and responsibility to make it work, and I can go to the Deputy Secretary and the Secretary as needed to identify problems, where in the past I did not have any clear authority. I could identify concerns, but I had no specific responsibility or authority. That has been clarified with the Deputy Secretary's memo of June 8.

Mrs. WILSON. What additional authority do you really have? Can you really tell DP or CR or EH or any of these little suborganizations, "Shut down your computer network until you fix the following problems?"

Mr. GILLIGAN. That is one of the new authorities that I have. With my ability now to enforce a connection policy, if that policy is not adhered to, I can and will shut down those organizations.

Mr. BURR [presiding]. If the Chair could ask the gentlelady to wrap up as quickly as she can, I think that it's only right to allow them the opportunity for a break in between the 1 o'clock session. So if you would wrap up as quickly as you can.

Mrs. WILSON. Thank you, Mr. Chairman. In fact, I think that probably concludes the things that I'd like to pursue in this forum, and I thank all of you for your time.

Mr. BURR. I thank the gentlelady. I didn't think she'd be quite that quick, but the Chair would ask unanimous consent for the record to remain open for the purposes of opening statements of any members that request to enter those and for additional questions of members.

Gentlemen, let me once again thank you on behalf of this committee. I hope all of you understand the seriousness that we not only take of the headquarters evaluation, but the findings within the last 48 hours of continuation of a breach of our security at our labs.

Our hope is that, Mr. Podonsky, you will move forward with—at some point with an audit of the classified areas of headquarters, and that we will have an opportunity to review that.

And my hope is, Mr. Gilligan, with this new responsibility, and that's the coordination of one plan for security at headquarters, that you will be successful in making sure that that's implemented in the fashion that you see appropriate.

My hope, General, is that at some point we can get one plan for the individual labs that you have and your team have the confidence in that it is secure.

With this, this hearing is adjourned.

[Whereupon, at 12:15 p.m., the subcommittee was adjourned.]